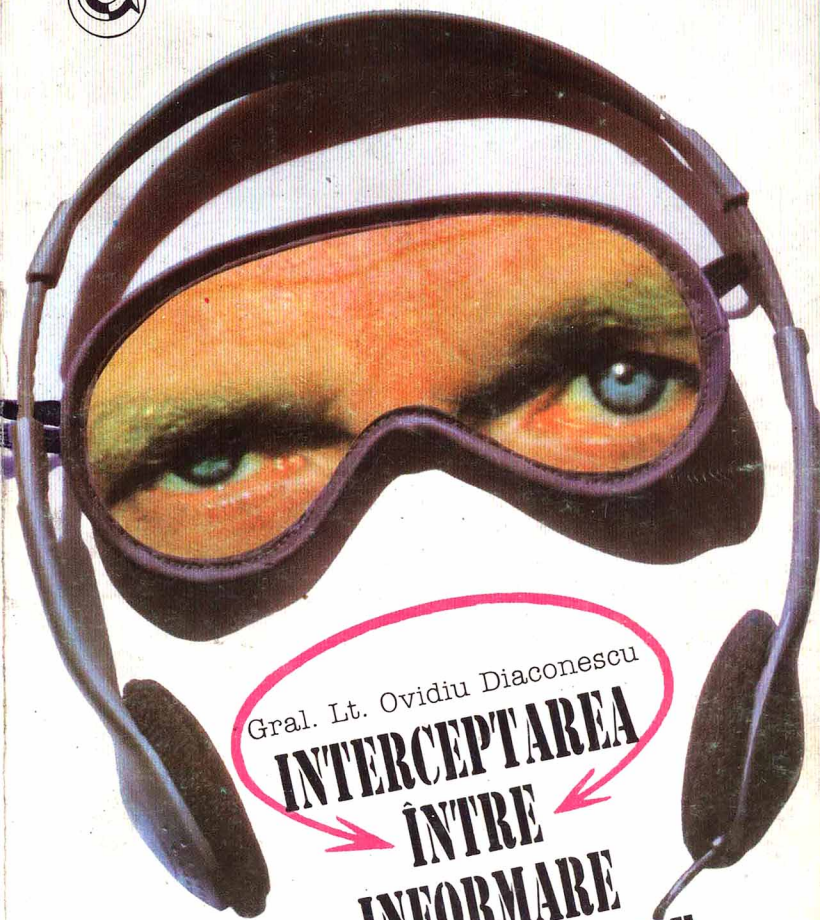




Gral. Lt. Ovidiu Diaconescu

INTERCEPTAREA

ÎN TRE

INFORMARE

ȘI DEZINFORMARE

G-ral. It (r) ing. OVIDIU DIACONESCU

**INTERCEPTAREA
INTRE
INFORMARE SI DEZINFORMARE**

Coperta: Gheorghe Baltoc
Redactor: Petre Bărbulescu

I.S.B.N. 973 - 49 - 0057 - 9

G-ral. lt. (r) ing. Ovidiu Diaconescu
INTERCEPTAREA
INTRE
INFORMARE SI DEZINFORMARE
© EDITURA GLOBUS
Piața Presei Libere nr. 1
71341 București, C.P. 18 - 33, Sector 1
Telefon: 618.08.82

G-ral. It (r) ing. OVIDIU DIACONESCU

**INTERCEPTAREA
INTRE
INFORMARE SI DEZINFORMARE**

**Tehnica
în
Spionaj - Contraspionaj**

**EDITURA GLOBUS
BUCURESTI**

C U P R I N S

	pag.
Cuvânt înainte	9
Capitolul I Spionaj - contraspionaj; mijloace și metode tehnice folosite	11
- Ce se înțelege prin tehnici de spionaj-contraspionaj	12
Capitolul II Scandaluri în lumea spionajului și contraspionajului	14
- Walt Disney desenator dar și spion	18
- Toate serviciile de informații folosesc tehnică specială	19
Capitolul III Interceptarea telefonică	32
- Apelul injurios sau cum se depistează cel ce apelează un telefon	33
- Se poate intercepta o națiune ?	35
- Interceptările telefonice neguvernamentale	37
- Ascultarea telefoanelor moderne o problemă facilitată	43
Capitolul IV Ne cunoaștem oare telefonul ?	51
Capitolul V Ascultarea convorbirilor interioare cu ajutorul telefoanelor și circuitelor lor	54
- Dispozitivul antifurt este în realitate un aparat de ascultare	54
- Organizarea și folosirea interceptărilor de către instituțiile guvernamentale specializate	56
- O secretizare superioară	61
- Ascultarea fără piese compromițătoare	62
Capitolul VI Interceptarea convorbirilor cu ajutorul microfoanelor și amplificatoarelor (microfon cu fir)	64
- Microfonul elementul de bază al interceptării	64
- Amplificatoare folosite în interceptări secrete	67
- Rețeaua electrică - suport ideal pentru interceptare	68
Capitolul VII. Microemițătoare - Microfoane fără fir	71
- Perfecționarea emițătoarelor pentru asigurarea securității interceptărilor	74
Capitolul VIII Dispozitive pasive	77
- Și familiilor regale le sunt interceptate convorbirile	79
Capitolul IX Interceptarea prin folosirea sistemelor direcționale optice - laseri	90

- Laser - raza morții dar și arma interceptării	92
Capitolul X Interceptarea informațiilor neauditive din sistemele de comunicații de date	97
- Vulnerabilitatea calculatoarelor	98
- Telexurile și telefaxurile se interceptează la fel ca telefoanele	100
Capitolul XI Metode și mijloace foto, chimice și electronice pentru transmis informații - soluții pentru depistarea acestora	102
- În patru milimetrii pătrați o pagină de informații	102
- Există și cerneală invizibilă	104
- Indigoul este uncori alb	105
- Spionii au în dotare emițătoare	108
Capitolul XII Mijloace și dispozitive optice și electronice pentru supravegherea fizică și înregistrarea imaginilor	112
- Aparate și mijloace pentru fotografieri secrete	112
- Optoelectronica și televiziunea în serviciul contraspionajului	115
- Localizarea emițătoarelor pentru depistarea persoanelor	118
- Depistarea emițătoarelor folosite în activități de spionaj - trădare	122
Capitolul XIII Metode și aparatură pentru depistarea interceptărilor telefonice, a altor sisteme de ascultare cu fir și de protecție împotriva acestora	127
- Interceptarea convorbirilor telefonice nu este infailibilă. Cum ne protejăm și cum o depistăm ?	128
- Mai bine cauți un ac în carul cu fân, decât un microfon într-o clădire	141
Capitolul XIV Detectarea dispozitivelor de interceptare radio (fără fir)	152
Capitolul XV Mijloace generale de protecție împotriva tuturor tipurilor de interceptări	160
- Camerele acustice din încăperi, botnițele și generatoarele de bruiaj	160
Capitolul XVI Perspectivile tehnicilor de interceptare, de supraveghere precum și a metodelor de neutralizare	171

Anexa I Utilizarea spectrului de frecvențe în S.U.A. și în unele țări occidentale	176
Anexa II Benzile de frecvență și denumirile lor	178
Anexa III Aparatura de interceptare românească după decembrie 1989	179
Anexa IV Ziariștii și sursele lor abordează problema tehnicii de interceptare	182
Anexa V Un scandal referitor la interceptarea convorbirilor în Spania	187
Bibliografie	195

CUVÂNT ÎNAINTE

O parte dintre cititori vor spune că am prezentat prea puțin din ceea ce se cunoaște că există în domeniul tehnicii folosite în activitățile de spionaj și contraspionaj; alții, din contră, vor zice că am spus prea mult. Cei care au temeinice și avansate cunoștințe în electronică și telecomunicații vor reproșa lucrării că nu intră în amănunte de specialitate, iar ceilalți s-ar putea să fie derânjați că se folosesc prea multe date tehnice.

Nu doresc să intru de la început în aceste dispute, deși, până la urmă, îmi voi spune părerea, ci, în primul rând vreau să amintesc tuturor cititorilor că este prima lucrare publicată în țară care abordează această temă și de aceea este foarte probabil, ca de altfel toate lucrările de pionierat, să nemulțumească pe unii, pe care îi invit, dacă au o altă viziune asupra problemei tratate, să și-o formuleze așa cum doresc, într-o nouă lucrare pe care publicul c va aprecia.

De ce am scris-o ? Am considerat că publicarea ei va umple un gol, că publicul larg cunoaște prea puțin, că trebuie spus adevărul, mai ales pentru că asupra acestor probleme, există din multiple cauze, la foarte multe persoane păreri deformate.

Fără să încerc să scuz abuzurile din ultimii cincizeci de ani din țările foste comuniste-socialiste prin folosirea tehnicii, în special cea de interceptare, împotriva unor persoane ce nu intrau în sfera de preocupare a spionajului sau a contraspionajului, ci din cu totul alte motive, am arătat însă că activități de informații și contrainformații - cu folosirea tehnicii corespunzătoare - s-au desfășurat de foarte mult timp, de către toate statele. Nici România nu putea face excepție și tehnica în slujba spionajului și contraspionajului, n-a început după 1945 și nici nu se va termina cu anul 1989.

Lucrarea nu poate intra în toate amănunțele tehnice pentru că tratează întregul domeniu, de la interceptările de toate tipurile, la transmiterea informațiilor, la cifrare, la tehnica de observare-supraveghere și în final la mijloacele și dispozitivele

necesare protecției, depistării, la contramăsurile împotriva mijloacelor tehnice ofensive.

Poate m-am referit în extenso la problema interceptării telefoanelor pentru că am considerat că aceasta interesează în mod special mai multe persoane.

Am apreciat că lucrarea de față nu se adresează numai specialiștilor în problemele tratate ci și publicului larg, dornic de informare-documentare care vrea să cunoască realitatea în materie. Acestui public, autorul își cere scuze și-l roagă să-l înțeleagă că n-a putut evita în tratarea problemelor termeni tehnici precum modulație, detecție, miliampermetre, serie-paralel etc. Sper că n-am deranjat prea mult acum, când suntem inundați cu termeni din lumea ordinatoarelor, a finanțelor ca: input, output, indexare, holding, limbaj, soft, f.o.b., dividende etc.

Celor care apreciază că am scris prea mult despre unele probleme pe care ei le consideră secrete aș dori să le spun că și în acest domeniu, al aprecierilor, s-au schimbat multe lucruri după decembrie 1989, că nu este secret mijlocul tehnic, cunoscut pe plan mondial, ci acțiunea în care este folosit, motivul întrebuintării și cum sunt exploatate rezultatele obținute.

Oricum, eu consider că toate afirmațiile pe care le-am făcut în lucrare au acoperire în publicațiile externe și interne din care m-am documentat.

Prezenta lucrare are o valoare specială pentru tinerii diplomați, oamenii de afaceri, ziariști precum și pentru cei ce doresc să se pregătească pentru munca de informații-contrainformații, ingineri și tehnicieni care vor să se specializeze în domeniul creării de aparatură specifică activității de obținere și transmitere de informații, de protecție și depistare a acestor mijloace și procedee tehnice.

Parafrazând o reclamă occidentală, doresc în final să mulțumesc viitorului cititor pentru alegerea făcută, procurându-și cartea, și-i urez împlinirea și satisfacerea dorințelor de a cunoaște cât mai mult din toate domeniile care îl interesează.

AUTORUL

CAPITOLUL I

SPIONAJ-CONTRASPIONAJ MIJLOACE ȘI METODE TEHNICE FOLOSITE

Mulți oameni de știință sunt de acord că printre elementele ce contribuie la dezvoltarea civilizației societății umane este și curiozitatea, acea dorință de a ști mai mult, de care au fost animate multe persoane. Necesitatea organică de a cunoaște tot ceea ce natura ori colectivități, instituții sau țări "apără", pe de o parte și dorința de a le proteja împotriva celor "indiscreți", pe de altă parte, determină una din cele mai puternice curse care se desfășoară în întreaga lume. Oare focul, în epoca de piatră, după ce a fost adus pe pământ nu s-a răspândit prin furarea secretului acestuia de la oamenii unei peșteri de către locatarii altele ? De aici până la constatarea că spionajul și contraspionajul sunt tot atât de vechi ca și istoria omenirii nu este decât un pas.

În această succintă lucrare nu ne propunem să facem o istorie exhaustivă a spionajului ci să prezentăm tehnica folosită în această activitate, ale cărei începuturi se plasează, așa cum spunea legenda, cu peste 30 de secole înaintea celebrei Mata Hari. Atunci Dalila i-a luat puterile supranaturale judecătorului evreu Samson, prin tăierea celor șapte șuvițe de păr și l-a predat Filistenilor, în slujba cărora ea a acționat. Acestea s-au întâmplat înaintea domniei lui Alexandru cel Mare care, pentru a ști ce gândesc și cum acționează generalii și ofițerii lui, a organizat prima interceptare în masă a corespondenței poștale trimisă de pe câmpurile de luptă, prin curieri, în țară.

Dacă este greu de stabilit cu precizie începutul acestei activități, la fel de greu este să reușești, dacă-ți propui, să nominalizezi care a fost cel mai mare spion, cel care a avut cele mai semnificative reușite, cel care a adus cele mai multe servicii cauzei țării sau idealului pentru care a acționat. Doi dintre aceștia pot concura la acest loc. Ei au fost, din întâmplare contemporani și au trăit în perioada celui de-al doilea război mondial. Este vorba, în primul rând, de Reinhard Heydrich, unul din ajutoarele doctorului Heinrich Himmler, cel care a condus mult timp S.D-ul german, însărcinat cu spionajul și contraspionajul politic al partidului nazist.

El a reușit, prin acțiuni de adevărat maestru, să-l "intoxice" pe Stalin, să-i sădească acestuia neîncrederea în conducerea Armatei roșii pe care în anii 1937-1938, practic, a și decimat-o. Așa se explică în bună măsură succesele Armatei germane, în primele luni, în războiul împotriva U.R.S.S.-ului. Că victoriile inițiale n-au putut fi continuate se poate explica și prin aceea că, în cealaltă parte a taberei, se găsea tot un mare spion, Richard Sorge care lucra pentru sovietici încă din 1925. Acesta a trimis Moscovei, cu luni de zile înainte, data exactă când Germania nazistă urma să atace U.R.S.S. Stalin nu l-a crezut, n-a luat măsurile necesare dar, după confirmarea datei începerii războiului, toate informațiile ce veneau de la Tokio, din partea rețelei conduse de Sorge, aveau prioritate și credibilitate maximă. Astfel, informația că Japonia nu va ataca U.R.S.S. a putut fi exploatată cu eficiență maximă prin retragerea diviziilor sovietice din Siberia, care apoi vor apăra și salva Moscova, acțiune ce a însemnat și sfârșitul războiului fulger purtat de armata hitleristă.

Ce se înțelege prin tehnici de spionaj - contraspionaj

Odată cu acumularea de noi cunoștințe în domenii de vârf ca electronica, fizica solidului, cu toată gama de semiconductoare, chimie organică, foto-optică, televiziune, astronautică, pe măsura perfecționării neconținute a ordinaroarelor și a tehnicii de calcul, a sistemelor de transmisie, munca de informații capătă dimensiuni noi, nebănuite.

În același timp, industria producătoare de tehnică de spionaj și contraspionaj înregistrează o adevărată explozie, cunoaște un real boom.

În secolul în care trăim, activitatea de informații și tehnica adecvată acesteia s-au contopit, ajutându-se și influențându-se reciproc. Astfel, Sorge n-ar fi putut fi un mare spion cu toate calitățile lui personale, dacă nu era dotat cu un emițător cu ajutorul căruia să-și transmită informațiile centrului de recepție din Siberia sovietică. De asemenea, demascarea lui n-ar fi fost posibilă, dacă organele de contraspionaj japoneze n-ar fi folosit ultimele modele germane de goniometre pentru localizarea transmisiunilor radio pe care acesta le efectua.

Prin tehnica destinată activității de spionaj și contraspionaj

trebuie să înțelegem metodele și aparatura destinate, în primul rând, interceptării discuțiilor purtate de persoane urmărite, incluzând între acestea și mult discutatele ascultări ale convorbirilor telefonice. Tot aici trebuie să încadrăm și aparatura și mijloacele necesare transmiterii informațiilor, atât pe cale electronică (emițătoare de diferite tipuri) cât și pe cale fotochimică (micropunct, scriere simpatică). Aparatura necesară cifrării și descifrării cu diferite grade de asigurare a secretului, a mesajelor transmise, cea pentru observarea și înregistrarea imaginilor pe peliculă foto sau videomagnetice este tot tehnică de spionaj și contraspionaj, la fel ca și satelitul-spion care determină mișcările trupelor, locul de unde se lansează rachete, sau de unde se efectuează explozii nucleare, interceptarea unor convorbiri telefonice, precum și a comunicărilor radio ale forțelor armate.

Toate acestea, în competiția la care ne-am referit la începutul lucrării, au reușit să creeze o industrie a metodelor de depistare, de anihilare, de bruieră a unora dintre mesaje, de criptare a altora, de localizare a emisiunilor radio, de depistare sau anihilare a microfoanelor ce sunt plasate într-o încăpere, de pază și alarmare. Procedeele din urmă, spre deosebire de primele care au un caracter ofensiv, le vom numi, pentru prescurtare, tehnică defensivă. Aparatura și mijloacele devin cunoscute publicului larg pe măsură ce se descoperă noi cazuri de spionaj, au loc noi abuzuri guvernamentale sau se schimbă regimuri politice și, odată cu prezentarea faptelor concrete, se descrie și tehnica folosită și depistată. Bineînțeles, când acestea sunt date publicității, pentru că trebuie spus că de cele mai multe ori, există o înțelegere tacită între serviciile de spionaj și contraspionaj adverse, de a nu se publica ceea ce se descoperă în acest domeniu. Astfel, în timpul războiului rece, tehnicile de interceptare, descoperite în ambasade, fie din fostele țări socialiste, fie din statele occidentale, de regulă, nu s-au prezentat public. De exemplu, România n-a anunțat niciodată la vremea respectivă că a descoperit emițătoare, microfoane sau telefoane modificate la unele din ambasadele sale din străinătate, după cum nici serviciile speciale occidentale n-au făcut caz de microfoanele descoperite în ambasadele sau locuințele diplomaților și specialiștilor lor, la București. Au fost însă și multe cazuri care s-au făcut publice sau de care autorul a luat cunoștință în alte moduri și la acestea se vor face referiri în continuare.

CAPITOLUL II

SCANDALURI ÎN LUMEA SPIONAJULUI ȘI CONTRASPIONAJULUI

Cititorii își amintesc de scandalul stârnit în 1956 atunci când purtătorul de cuvânt al trupelor de ocupație sovietice din Berlin a prezentat presei internaționale tunelul, cablurile și echipamentul folosite de Armata americană din Germania pentru a intercepta convorbirile telefonice din rețelele folosite de trupele sovietice. În continuare, nu vom respecta ordinea cronologică și vom începe cu cele publicate în anii 1970, pentru că atunci s-au discutat, foarte mult, problemele și implicațiile interceptărilor convorbirilor realizate la nivel guvernamental de către organizații specializate, precum și alte acțiuni de spionaj și contraspionaj în care s-au întrebuințat mijloacele tehnice. Să începem prin a aminti de afacerea "Watergate" când C.R.E.E.P.- Comitetul pentru realegerea lui Nixon în 1972 la Casa Albă - pentru compromiterea campaniei de alegeri a Partidului Democrat - a crut, în cadrul acțiunii "Operation Gemstone", în mai 1972, lui James McCord, lui Gordon Liddy și lui Everete H. Hunt, foști agenți C.I.A. și F.B.I., să instaleze dispozitive de interceptare, atât a convorbirilor, ce se purtau prin telefon cât și a celor ce aveau loc în încăperile statului major al Partidului Democrat, din clădirea complexului Watergate din Washington.

Intrând din nou în aceste apartamente, la 7 iunie în același an, pentru unele reorientări și reparații ale aparaturii, respectivii agenți au fost arestați de sergentul de poliție Paul Leeper, considerându-se la început, că aceștia erau spărgători. De aici, scandalul declanșat de doi ziariști, Carl Bernstein și Bob Woodward de la "Washington Post", cu urmările arhicunoscute, asupra cărora nu vom mai insista.

În 1973, un magistrat italian, dr. Luciano Infelise anunța că pe baza investigațiilor sale a descoperit vaste rețele de interceptare care afectează păături largi ale populației. Aspecte asemănătoare, tot în cazul interceptărilor telefonice, s-au petrecut în același an și în Anglia și Franța. Din ultima țară s-au publicat și fotografiile ale aparaturii de supraveghere din centrala operațională a Grupului Interministerial de Control (G.I.C.), precum și detaliile

privind un aparat destinat identificării numerelor de telefon solicitate de posesorul celui supravegheat. Am ales la început aceste exemple, datorită faptului că au fost, poate, printre cele mai importante, dar și pentru a demonstra că și în țări cu vechi tradiții democratice au avut loc abuzuri, s-au folosit și se mai utilizează astfel de instalații de interceptare. Desigur, se mai pot da și alte exemple în acest sens. Putem arăta că în anii '50 organele de contrainformații americane au descoperit în stema S.U.A., care fusese oferită ambasadorului american de către statul sovietic, dispozitive de ascultare cu care au fost interceptate convorbirile purtate de acesta în biroul său de la Moscova.

Reprezentantul S.U.A. de la Națiunile Unite, Cabot Lodge, a prezentat stema cu explicațiile necesare într-o sală, în Palatul Națiunilor Unite de la New York. Organele specializate americane, au descoperit în 1964, 40 de microfoane instalate de K.G.B. și care, au funcționat mulți ani în ambasada americană de la Moscova.

Ofițerul de contrainformații al S.U.A. au dejucat în 1966 și apoi au publicat cu toate datele și fotografiile necesare, încercarea a doi diplomați dintr-o țară est-europeană de a plasa un dispozitiv de interceptare (un microemițător mascat într-o bucată de lemn) într-un birou al Departamentului de stat american de la Washington. În literatura de specialitate s-a publicat știrea că organele de pază și control tehnic ale Ambasadei S.U.A. de la București au depistat un microemițător montat în tocul unui pantof bărbătesc. Nu s-au dat alte amănunte, decât aprecieri pozitive asupra calității deosebite a microemițătorului și stabilirea faptului că acesta era de fabricație românească. Si, pentru că ne-am referit la țara noastră, trebuie să arătăm că în ultimul timp s-au publicat date și documente de arhivă care atestă, fără putință de tăgadă, că încă de la primele construcții de centrale telefonice s-au prevăzut, instalat și adaptat, dispozitive de interceptare a convorbirilor telefonice.

În anul 1934 (și-a în vigoare Constituția din 1923) s-au purtat discuții aprinse în Adunarea Deputaților privind interceptările ce se făceau la Palatul Telefoanelor din Calea Victoriei și în Centrala din Bd. Dacia, în mod organizat, sistematic și cu aparatură modernă pentru acele timpuri. Armand Călinescu, un politician care nu poate fi acuzat că nu era în miezul problemelor și care a fost și șeful serviciului informativ al P.N.T.,

relatează în "Însemnări politice" despre interceptările care se făceau în acea perioadă ca despre niște probleme diverse, obișnuite. S-au publicat stenograme ale unor interceptări telefonice de la începutul anului 1938 în care întâlnim numele unor oameni politici la care ne referim și astăzi ca Iuliu Maniu, Virgil Madgearu, Nicolae Titulescu, Corneliu Coposu etc. Poate aceste discuții se datorau și faptului care era de notoritate publică, că Elena Lupescu avea propriul serviciu de informații, avându-l ca ajutor direct pe domnul Pitulescu, director al Poștei și Telefoanelor, deci cel care avea pâinea și cuțitul în problema interceptărilor telefonice și poștale.

Deși serviciile de informații și de siguranță ale țării au suferit în 1940 lovituri puternice, deoarece germanii naziști și Legionarii făcuseră tot ce le stătuse în putință pentru a le dezorganiza și a pune mâna pe documente, arhivă și în special pe listele cu agenți, interceptările telefonice au continuat toată perioada 1940-1944. Din articolele publicate în "Magazin istoric" nr. 7 și 8/1993, pe baza memoriilor lt.col. Traian Borcescu din S.S.I. (chiar șeful acestuia pentru perioade foarte scurte, după arestarea lui Eugen Cristescu - director S.S.I. până la 23 august 1944); reiese clar că, S.S.I.-ul a interceptat convorbirile regelui și a reginei mamă.

De asemenea, din publicarea jurnalului lui Ion Hudita fruntaș național-țărănist - reiese că acesta, prin indiscreția unui funcționar de la Președinție, pe numele său Radulescu a aflat că Ion Antonescu a primit un dosar de la același Eugen Cristescu cu anexe ce conțineau convorbirile telefonice ale acestuia cu o serie de personalități militare. Ion Hudita - secretar general adjunct al P.N.T. - într-o audiență la Mihai Antonescu - vice-președintele guvernului - nu s-a plâns de interceptarea convorbirilor telefonice ci de interpretarea pe care directorul S.S.I.-ului a dat-o acestora și anume intenția de lovitură de stat cu ajutorul unor conducători militari (avusese loc lovitură mareșalului Badoglio în Italia). Odată cu capitularea de la 23 august 1944, S.S.I.-ul primește noi lovituri din partea serviciilor secrete aliate, în special sovietice, prin intermediul lui Emil Bodnăraș, dar și americane, care au obținut multe documente secrete preluate de la Mocsonyi - Stârcea și predate lui Ivor Porter. Cu toate acestea interceptările continuau. După 1944, mijloacele de interceptare au fost preluate, dezvoltate și modernizate de către organele de stat și folosite atât pentru

apărarea națională, cum a fost descoperirea fostului general I. Serb ca spion sovietic - care telefona de la cabină publice la reprezentanții din București ai comandamentului forțelor armate unite (C.F.A.U. - Tratatul de la Varșovia), dar, din păcate, și împotriva multora care nu aveau altă vină decât aceea că și-au exprimat dezacordul total sau parțial față de putere (anexa a III-a).

N-au trecut neobservate și s-a făcut multă publicitate încercărilor de supraveghere și fotografiere din anii 1955-1956, cu ajutorul baloanelor de spionaj, pe care S.U.A. le lansa din Nordul Europei. Acestea străbăteau vestul și centrul Uniunii Sovietice, la 10 mii de metri înălțime și apoi aterizau în Turcia, Nordul Africii, sau amerizau în Marea Mediterană ori în Marea Neagră.

Câteva zeci dintre ele au căzut și în România, în sudul Moldovei, în Delta Dunării și în nordul Dobrogei. Aceste baloane erau dotate cu aparatură sofisticată, în primul rând fotografică, care realiza, de la înălțimea de 10 km, pelicule în care, după dezvoltare, se puteau distinge clădiri, posedau dispozitive care trebuiau să mențină constată înălțimea de survolare prin aruncarea de balast, când balonul pierdea înălțime, aparatură care poziționa locul de unde s-a executat fiecare fotografie și marca ora la care aceasta a fost realizată.

Se aflau foarte multe accesorii, dintre care amintesc numai emițătorul de semnal (baliză) care intra în funcțiune după aterizare sau amerizare, pentru a putea fi localizat cu ajutorul goniometrării, în vederea recuperării filmelor, singurele care prezentau interes.

Reamintim cititorilor noștri scandalul diplomatic produs de doborârea avionului de recunoaștere U2, pilotat de Gary Powers care în anul 1960 survola la o înălțime de peste 30 km, teritoriul sovietic. După îmbunătățirea relațiilor ruso-americane, presa a adus la cunoștința opiniei publice că s-au efectuat sute de zboruri și că americanii au pierdut foarte mulți piloți în aceste activități aeriene de spionaj. Să nu uităm "valurile" declanșate de capturarea, în 1968, de către nord coreeni, a vasului de spionaj american Pueblo, destinat interceptării convorbirilor telefonice. La începutul anilor 1980, presa occidentală era plină de reproșuri ce se adresau organelor sovietice, datorită bombardării cu unde electromagnetice de foarte înaltă frecvență, a Ambasadei americane, în vederea "activării și alimentării" unor dispozitive

pasive de interceptare a convorbirilor. După 1985 odată cu "dezghețul" în relațiile ruso-americe, a izbucnit și un mare incendiu în clădirea Ambasadei S.U.A. de la Moscova, iar problema a rămas nelămurită.

Deși s-au produs multe scandaluri și din aceste cauze au căzut multe capete politice (Richard Nixon) totuși în domeniul spionajului și contraspionajului, a avut loc o dezvoltare continuă a mijloacelor și s-au folosit tehnici din ce în ce mai sofisticate.

Cine și-ar fi imaginat că, la sfârșitul anilor '80, F.B.I. va aresta un cetățean american, care în final va fi condamnat pentru spionaj în favoarea statului Israel. Prietenia este prietenie, dar afacerile sunt afaceri.

Cotidianul spaniol "El Pais" nr. 5846 din 1 Mai 1993 publică, la pag. 40, articolul "*C.I.A. acuză Franța că a practicat spionaj industrial împotriva sa*". Din conținutul articolului semnat de Javier Valenzuela, rezultă că C.I.A. a acuzat Franța că a practicat un spionaj industrial sistematic împotriva întreprinderilor, băncilor și ministerelor din S.U.A., recomandând fabricanților nord-americani să nu participe, în luna iunie 1993, la Salonul Aerospațial "Le Bourget".

Walt Disney desenator dar și spion

Ne imaginăm ce șoc a produs în opinia publică mondială știrea că și binecunoscutul Walt Disney a fost implicat în activități de spionaj. Iată ce scria cotidianul italian "La Repubblica" din 7 mai 1993, la pagina 24 în articolul intitulat "Walt Disney - spion al F.B.I.-ului", semnat de Ennio Caretto: "Este o traumă pentru Hollywood, pentru America și pentru copiii și foștii copii din întreaga lume, care cresc sau au crescut în cultul desenelor animate: s-a descoperit că Walt Disney, creatorul lor, a fost un spion al F.B.I.-ului timp de 30 de ani, din '36 până în '66 când a murit și care, din '54 a avut gradul de S.A.C. ori agent special pentru contacte". Disney n-a fost un colaborator inofensiv al poliției federale: în perioada cea mai întunecată a istoriei moderne a Statelor Unite, vânătoarea de vrăjitoare comuniste din anii '50, el a denunțat zeci de colegi din cinema, poate mai mulți, pentru așa-zise activități subversive ori antiamericane, ruinându-le viața sau cariera. Si opera clandestină a lui Disney, de agent secret al regimului, în contrast cu candoarea și umanismul personajelor

sale, nu a fost solitară. Printre tovarășii lui excelenți se numără și Ronald Reagan, angajat al F.B.I. cu un rang inferior: în '47, când viitorul președinte al S.U.A. conducea sindicatul actorilor, figura abia ca "ST 10" ori sursa "T 10", adică informator de încredere.

După părerea lui Marc Eliot, un istoric al culturii pop, Walt Disney a conceput legătura sa cu F.B.I.-ul ca un angajament pe viață. Disney nu era magul cel bun din fabule: din punct de vedere politic, aparținea extremei-drepte.

Herbert Hoover, director al F.B.I.-ului, i-a conferit lui Disney titlul de S.A.C. în '54. Un agent special pentru contacte este mult mai mult decât un spion: este autorizat să folosească aparate de înregistrare, transporturi și alte echipamente pentru F.B.I. și să îndeplinească funcții de purtător de cuvânt. După doi ani Disney, i-a restituit favoarea: i-a pus la dispoziție Disneyland-ul, nu numai pentru primiri, ci și pentru probleme oficiale.

Cel mai mare parc de divertisment din lume conține un post de poliție ascuns ori un centru de spionaj! Din favoare în favoare, Hoover îi permite lui Disney să filmeze unele scenarii televizate în "santa sanctorum", clădirea F.B.I.-ului din Washington.

Este posibil ca dezvăluirile să aibă urmări răsunătoare. Administrația Clinton vrea să schimbe legea privind secretul de stat și, dacă se reușește, F.B.I.-ul, C.I.A. și Pentagonul ar fi obligate să deschidă pentru public mult mai multe dosare decât le convine.

Din celelalte dosare, deschise până acum, s-a aflat că Poliția Federală îi ținea sub supraveghere pe toți, câte puțin, de la Elvis Presley la Beateals și că avea alți informatori iluștri, pe lângă Disney și Reagan. Dar, în anii petrecuți la Casa Albă, Reagan a susținut că a colaborat cu F.B.I.-ul numai împotriva corupției.

Toate serviciile de informații folosesc tehnică specială

Este greu să se renunțe, din rațiuni legale sau morale, la mijloace eficiente de procurare a informațiilor deosebit de utile, mai ales când este vorba de apărarea siguranței naționale, de depistarea unor spioni care acționează împotriva țării lor, de prindere a unor criminali sadici, pentru curmarea activității

neșăbuite la unor răpitori de copii în schimbul cărora solicită mari sume de bani, sau pentru obținerea de date care să ducă în final la capturarea unor grupări teroriste.

Intr-o lucrare publicată în Franța, în anul 1985, diplomatul Jacques Baeyens ne arată că nu sunt simple supoziții ascultarea telefoanelor unor diplomați în țările în care aceștia își desfășoară activitatea. Nu mijloacele și procedeele tehnice pot fi acuzate, ci modul cum acestea sunt folosite. Una este să fie întrebuințate în scopurile la care m-am referit și alta este să fie folosite pentru a obține informații de la conducătorii partidelor de opoziție, sau de la alți adversari politici, (exemplu Watergate). Este sigur că, din rațiuni înalte, în anumite limite, pentru unele scopuri, cu aprobările necesare și chiar cu unele excese și abuzuri, C.I.A. și F.B.I.-ul în S.U.A., Biroul 2, Direcția supravegherii teritoriului și S.D.E.S.E. (organul de spionaj francez), K.G.B.-ul și G.R.U. - sovietic, S.I.S. (Secret Intelligent Service) și M.I. 5 englez, precum și altele au folosit și folosesc mijloace de interceptare, de observare, de fotografiere secretă, de transmitere a informațiilor etc.

În general, toți cei care au analizat problema interceptărilor telefonice au căzut de acord că, și în țări cu vechi tradiții democratice, există situații în care, pentru scopurile pe care le-am arătat mai sus, serviciile de apărare a siguranței statului organizează activități de interceptare. Un stat modern și dezvoltat care are în structura sa servicii de informații (de spionaj și contraspionaj), trebuie să posede și să folosească și tehnica adecvată acestor scopuri. Datorită campaniei împotriva acestor interceptări de telefoane, dusă în țară, după decembrie 1989 sunt tratate în extenso aceste probleme. În loc să se condamne abuzurile, încălcările, modul ilegal în care au fost folosite în multe cazuri, ura s-a revărsat mai mult asupra mijloacelor tehnice care, practic, au fost demolate așa cum în secolul al XIX-lea, muncitorii din Lyon au distrus războaiele de țesut. N-au trecut însă, nici doi ani și prin "Legea siguranței naționale a României", în art. 13, s-au stabilit condițiile și aprobările necesare pentru folosirea lor. Pentru detalii se recomandă anexa a III-a.

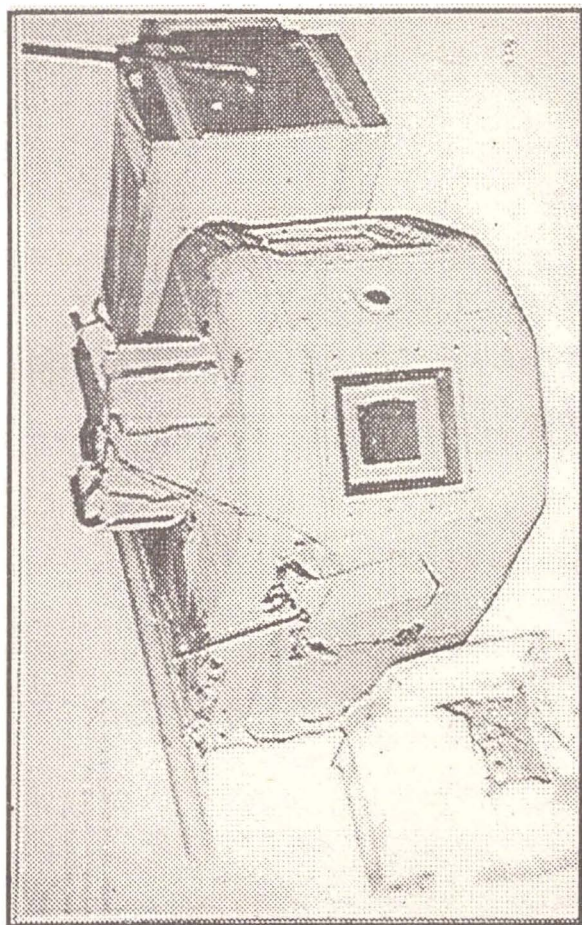
Pentru documentarea cititorilor prezentăm pe scurt cum este reglementată, cel puțin oficial, și ce se prevede în legislație privind interceptarea convorbirilor telefonice în unele țări europene. Astfel, în cotidianul belgian "Le soir" din 25 iunie 1993 a apărut articolul "Ascultările telefonice sunt ilegale, dar...", din



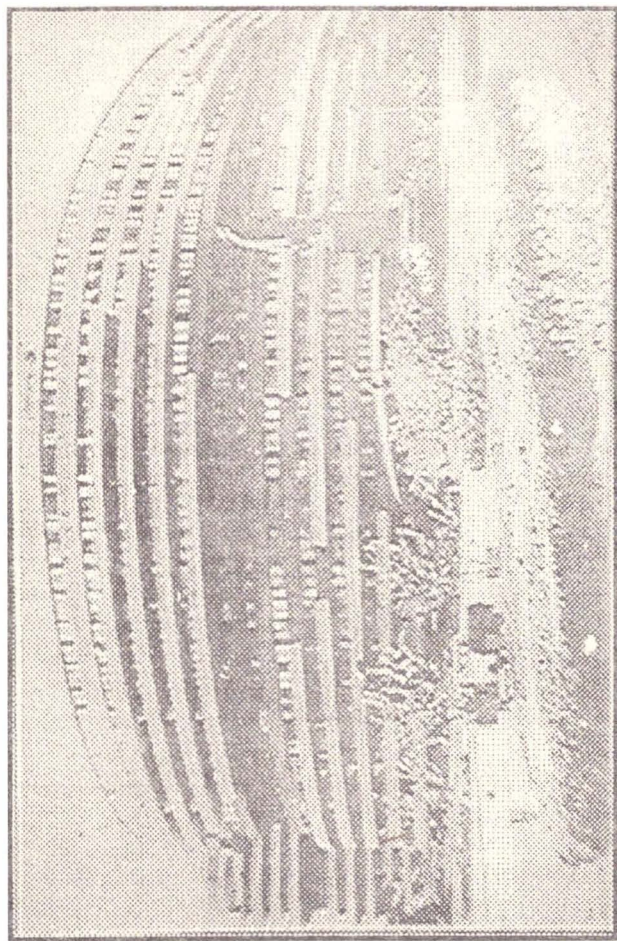
Ofiterii sovietici prezinta presei, in 1956, tunelul, cablurile si aparatura folosite de armata americana pentru interceptarea convorbirilor telefonice ale trupelor sovietice de ocupatie din Berlin.



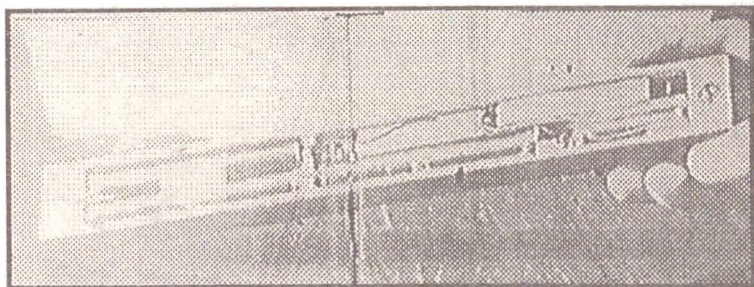
Intr-o sala a cladirii O.N.U. de la New York se prezinta stema scoasa din ambasada S.U.A. de la Moscova si in care a functionat un dispozitiv de interceptare montat de K.G.B.



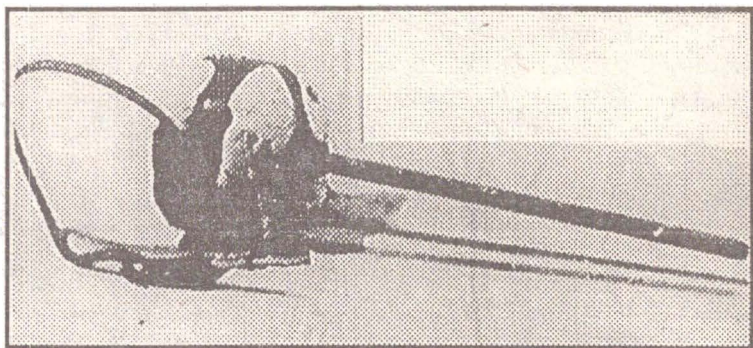
Unul din baloanele de spionaj care a strabatut la sfarsitul deceniului cinci, spatii ale unor tari din estul Europei, in special ale fostei U.R.S.S.



Cladirea Watergate din Washington, unde a avut loc scandalul care a dus la caderea presedintelui Nixon.



Emitator plasat într-un penar de lemn, pe care în 1966, diplomați cehi au încercat să-l plaseze în clădirea Departamentului de Stat al S.U.A. din Washington.



Microfon dinamic, cu tub acustic, dintre cele 40 care au fost scoase din clădirea ambasadei S.U.A. din Moscova

care redăm selectiv:

"Ascultările telefonice au fost întotdeauna obiectul unor reglementări specifice în toate țările Comunității Europene. Belgia încearcă să rezolve această întârziere în cadrul Consiliului miniștrilor care trebuie să se pronunțe asupra unui proiect de lege al ministrului Walhelet. Elementul esențial îl constituie interzicerea ascultărilor telefonice cu excepția anumitor cazuri bine determinate."

"În virtutea unei circulare ministeriale ce datează din 17 august 1923 agenții poliției judiciare și de la serviciile secrete (ex. B.S.R.) pot brânșa pe o linie mijloacele de ascultare, care să le permită să știe cine a sunat un suspect și pe cine a apelat acesta. Curtea de Casație a apreciat prin hotărârea din 2 mai 1990 că acest procedeu era ilegal."

"Astăzi un proiect de lege modificat va trebui să fie analizat în Consiliul de miniștri. În prima parte, proiectul prevede adăugarea la Codul Penal de sancțiuni pentru agenții care ascultă sau pun pe alții să asculte comunicații la care ei nu iau parte direct; idem pentru cei care instalează dispozitive în acest scop; ca și pentru cei care dețin, relevează sau divulgă informații culese prin aceste procedee. Reglementarea prevede și pedepse mai severe dacă acest lucru se face cu intenție, în mod fraudulos".

Apoi proiectul propune inserarea în codul de procedură penală a circumstanțelor în care excepțiile la interzicere pot fi acordate: < < Atunci când necesitățile o impun, judecătorul de instrucție poate, cu titlu excepțional, să asculte, să ia cunoștință de text sau să înregistreze comunicații în cazul în care există indicii serioase și când alte mijloace de investigație nu sunt relevante pentru depistarea adevărului. > >

În presa germană întâlnim titluri: "*Kohl vrea mai multă putere pentru poliție*". Iată ce scrie un cotidian:

"Confruntată cu un terorism activ, Germania autorizează ascultările telefonice în anumite cazuri foarte precise, decise prin lege: pericol pentru securitatea statului, pentru instituțiile democratice. Adoptată înaintea reunificării, legea reflectă una din îngrijorările principale ale epocii: pericolul unei infiltrări comuniste. Punerea sub ascultare este posibilă și în cazuri de delictе financiare importante. Totuși, ea nu se poate efectua decât în condiții foarte precise: un judecător de instrucție să dea autorizația. Protecția libertății individuale fiind foarte puternică în

dreptul german, poliția s-a plâns în mod constant că nu are mijloace de luptă eficace și nu poate interveni repede. U.C.D. (Uniunea Creștin Democrată) - partidul cancelarului Helmut Kohl - ar vrea să propună parlamentului o lege care să acorde puteri sporite poliției..."

În Anglia ceea ce se scrie despre această problemă se poate rezuma sub titlul: "Dispozitive care fac ca legea să fie învechită." Parcurgându-le aflăm următoarele:

"Un gentelman nu ascultă conversațiile altuia. În virtutea acestei vechi și nobile zicale engleze, o lege votată în 1985 <<Interceptions Communications Act>> interzice teoretic punerea sub ascultare. Dar pentru a lupta împotriva unor oameni care nu se comportă ca niște gentelmen acest frumos principiu are unele excepții: <<imperativele de securitate națională, de luptă împotriva terorismului sau împotriva traficului de droguri>>".

"Pentru a putea înregistra conversațiile unui suspect este necesară autorizarea unui magistrat".

"Ingineri de la British Telecom, special pregătiți, sunt însărcinați cu administrarea".

"Se apreciază că în fiecare an sunt în mod oficial înregistrate 35000 de conversații. Dar în practică reglementarea este încălcată prin folosirea de <<microfoane secrete>>, de dispozitive speciale care permit celor care nu sunt gentelmen să înregistreze convorbirile telefonice."

În Italia, referitor la aceeași problemă, din presă reținem următoarele:

"Ministerul Public - un magistrat - trebuie să facă cerere la un judecător pentru anchete preliminare (GIP) atunci când apreciază că ascultările sunt indispensabile pentru ancheta sa: atunci când este vorba de delikte care sunt pedepsite cu o detenție cu închisoarea de peste 5 ani - sau delikte legate de contrabanda sau traficul de stupefiante sau de arme - sau când telefonul este utilizat pentru a comite un delikt (amenințări prin telefon, apeluri ale unor maniaci sexuali etc.)".

"Permisul nu poate fi obținut decât pentru 15 zile și poate fi reînnoit".

"Rezultatele sunt înregistrate și apoi retranscrise și trebuie să figureze într-un registru special."

"Ele pot fi ascultate de către apărătorul inculpatului. În

caz de urgență, Ministerul Public se poate dispensa de autorizația GIP pe o perioadă de 24 de ore".

"Responsabilii pentru lupta antimafia sau antiterorism beneficiază de puteri speciale pentru a organiza ascultările, evitând această procedură".

În presa olandeză găsim:

"Conform legislației olandeze, poliția este autorizată să efectueze ascultări telefonice în cazul în care ancheta poliției este avansată, cu aprobarea judecătorului".

"Această metodă de investigație este folosită în mod unic atunci când afacerea este apreciată <<foarte urgent>> sau când ancheta se găsește la un punct decisiv. Ascultarea este autorizată atunci când este vorba de un delict <<serios>>, pasibil de o pedeapsă de 4 ani închisoare".

"Poliția din Amsterdam declară că ascultările telefonice sunt o metodă frecvent utilizată".

"Când considerăm că este singura cale de a avansa, facem apel la un judecător de instrucție. Dar trebuie ca întotdeauna să ne justificăm cererea - explica un purtător de cuvânt".

"Proiectul de lege aflat actualmente în discuție revizuieste ansamblul procedurilor de anchetă și sugerează modificări în legislația ascultărilor".

"Ele n-ar mai fi autorizate decât pentru <<delicte grave>>".

Să vedem cum se prezintă situația în Franța, țară cu vechi tradiții democratice, unde cu ajutorul revistei "Science et vie" (iunie 1992) avem și cele mai bogate date din care redăm succint următoarele: Franța este o țară care a reprezentat, poate, cel mai tipic exemplu de folosire a interceptărilor într-o perfectă ilegalitate oficială, derularea acțiunilor specifice de acest gen realizându-se de-a lungul a peste 30 de ani, doar în baza unei circulare secrete emisă de Michel Debré în 1965. Pe această bază a funcționat, într-o cvasi-clandestinitate, Gruparea Interministerială de Control (G.I.C.), care își desfășoară și în prezent activitățile într-o clădire din Bulevardul Tour de Moubourg nr.51 bis, Paris 7 și este conectată la cel puțin 50 de centre de tranzit ale Parisului cu împrejurimile sale. Cum se știe, sunt mai multe centre de tranzit, probabil că sunt și alte locuri de interceptare ținute în secret.

Dispozitivul din provincie este descentralizat, funcționând

peste 120 de centre de ascultare a convorbirilor telefonice.

În cartea sa, "Cu cărțile pe masă", Michel Poniowski arată că, pe vremea când el era ministru de interne, ascultările se efectuau asupra: jurnaliștilor, conducătorilor sindicali și oamenilor politici, membri ai cabinetului ministerial și chiar miniștri. Candidații la alegeri se aflau sub supravegherea telefonică și chiar simpli cetățeni, sub pretextul sondajului de opinie.

În 1975 procedura de interceptare a devenit mai severă, prin intervenția președintelui Giscard D'Estaing care descoperise că fusese ascultat pe vremea când era prim-ministru de către Georges Pompidou care, pe de altă parte, declara tendențios că "un stat nu se dirijează ascultând pe la uși".

Lăsată de la un guvern la altul, dar niciodată votată, Legea care reglementează ascultările telefonice a fost adoptată, în sfârșit, la 10 iulie 1991, conferind o existență legală G.I.C.-ului și interceptărilor.

Conform dezvăluirilor din martie 1992 în centrul G.I.C. sunt autorizate 1180 posturi de ascultare care funcționează simultan, la care se adaugă un număr nelimitat și necontrolabil de radiotelefoane interceptate, de centrale fixe sau mobile de ascultare.

Dat fiind timpul limitat al interceptării, în decursul unui an, sunt trecute prin cele 1180 de linii, mii de posturi. Legea permite serviciilor speciale să suplimenteze substanțial numărul posturilor ascultate, în cazul când au loc evenimente deosebite - terorism, spionaj, subversiune, război.

Noua lege nu a făcut decât să oficializeze existența ascultărilor centralizate, administrative, botezate "interceptări de securitate".

Ea stabilește la patru luni durata maximă de punere sub interceptare, durată ce poate fi prelungită prin reluarea întregii proceduri, reținută într-un raport ce reprezintă un prețios instrument de control pentru Comisia pentru drepturile omului care prevede "că interceptările trebuie să aibă o durată rezonabilă".

Comisia de control a fost creată prin Legea din 1991, inspirată din Comisia Națională de Informatică și Libertate (C.N.I.L.) și se compune dintr-un președinte, desemnat de șeful statului dintre patru nume propuse și din doi parlamentari, dintre care unul este al opoziției.

Legea a fost elaborată la intervenția Curții Europene

pentru Drepturile Omului. La 24 aprilie 1990, Curtea Europeană - condamnase Franța pentru anumite proceduri de interceptare.

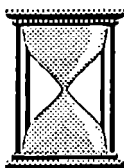
Nu e lipsit de semnificație și interesant de relevant faptul că, în Franța, printre instituțiile abilitate să beneficieze de interceptările telefonice sunt: Ministerul Apărării, Ministerul de Interne, Direcția Generală a Securității Externe (D.M.S.E.), spionajul francez, Direcția Protecției și Securității (D.P.S.D.), Ministerul Finanțelor, pentru vamă și T.R.A.F.C.I.N. (Tratament și Acțiune contra Circuitelor Financiare Clandestine) și nu în ultimul rând, Direcția supravegherii teritoriului (D.S.T.) - vestitul Contraspionaj francez.

Legea din 1991 autorizează și alte interceptări mult mai numeroase în afară de cele administrative, așa-numitele interceptări judiciare, asimilate "actelor de informare utilă în aflarea adevărului", dar le stabilește foarte strict condițiile, în sensul că doar instanța a fost abilitată să le autorizeze, prin judecătorul de instrucție și Comisia rogatorie.

O interceptare poate fi hotărâtă imediat ce apare o informație, dar numai dacă pedeapsa aplicată faptei este cel puțin de doi ani închisoare. Numărul simultan al acestor interceptări judiciare variază după diferite surse între 6000 și 20000 pentru verificarea și clasificarea celor 70 de mii de informații deschise pentru identificarea autorilor unor delikte grave.

Studierea atentă a centrului de interceptare de la Paris (C.I.G.), așa cum este descris în revista la care m-am referit, a datelor și fotografiilor prezentate, ne dă posibilitatea să arătăm în continuare cum se realizează o interceptare telefonică și cum funcționează un centru modern de ascultare.

Suntem convinși că la fel, cu mici deosebiri, neesențiale, sunt organizate aceste centre în toate capitalele țărilor care au posibilități tehnice și forță organizatorică.



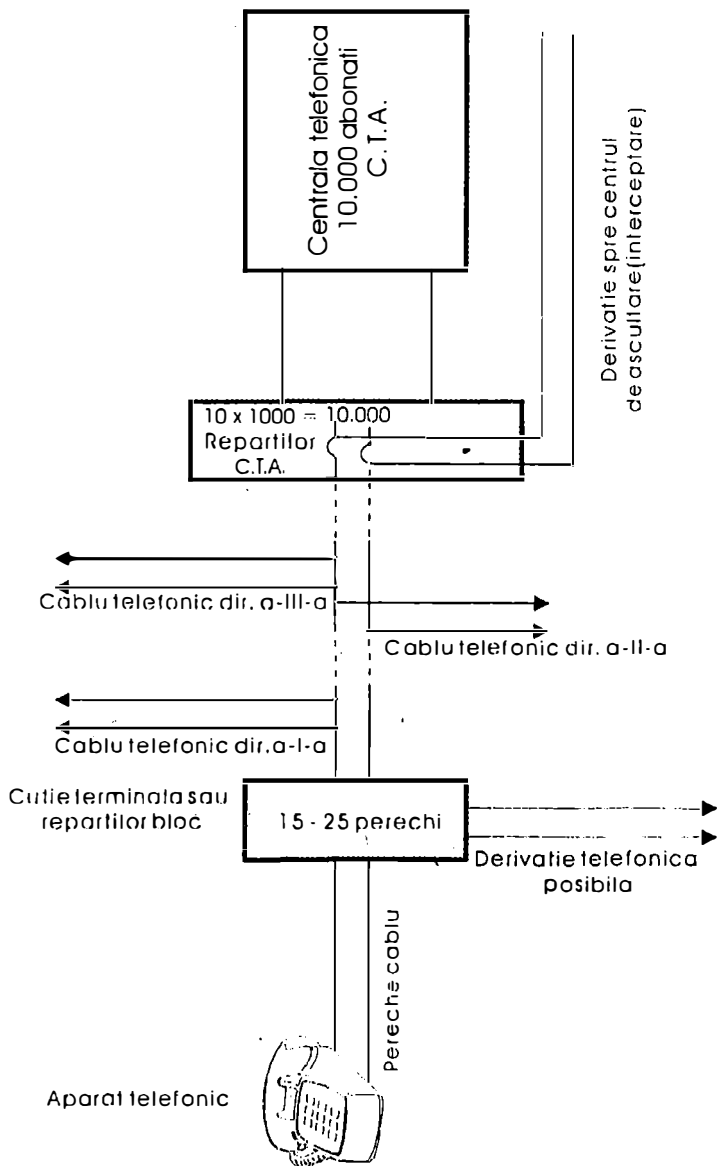


Fig. 1. Derivatii pentru interceptari telefonice

CAPITOLUL III

INTERCEPTAREA TELEFONICĂ

Intr-o cameră a unei clădiri, de cele mai multe ori secretă, un operator în fața unei mese pupitru, poate realiza interceptarea a 30-50 de posturi telefonice. În aceeași clădire, pot exista 20-30 astfel de încăperi dotate corespunzător, necesare pentru interceptarea a 600-1500 abonați telefonici.

Clădirea respectivă este legată prin cabluri telefonice cu toate centralele automate ale orașului (C.T.A.). Astfel, dacă se dorește interceptarea unui post telefonic, se procedează foarte simplu, conectând o pereche de fire din cablurile care leagă C.T.A. de Centrul operațional de interceptare, peste firele (în paralel), cu care, în repartitorul general al centralei telefonice automate (C.T.A.) este legat și telefonul ce urmează să fie interceptat (fig. 1). Astfel, acest post telefonic este bransat atât în C.T.A., dar și "tras" la una din mesele pupitru unde mai sunt conectate alte 29-49 telefoane. În momentul când se ridică microreceptorul telefonului dinspre C.T.A. circulă spre telefon un curent de câțiva zeci de miliamperi, situație care este sesizată tehnic la masa pupitru prin aprinderea unui bec pentru a semnaliza operatorului începerea convorbirii și automat, prin dispozitive speciale pornește și magnetofonul propriu fiecărui post telefonic.

Operatorul, prin apăsarea unui buton, intră pe circuitul acestui post ce se pregătește pentru convorbire și, prin acționarea unui dispozitiv, poate afișa numărul abonatului telefonic pe care îl formează cel care este interceptat. Când el dorește, poate asculta discuția care se poartă, dar aceasta în mod automat se și înregistrează pe bandă magnetică. Dacă din convorbire rezultă lucruri deosebite (întâlniri, se pun la cale acțiuni periculoase etc.), se anunță operativ cei interesați în problemă.

În cazul în care convorbirea este banală, se poate comanda întreruperea înregistrării concomitent cu marcarea unui semnal care să arate că oprirea a fost voită și nu accidentală.

Am arătat că, dacă dorește, operatorul, folosind un dispozitiv electronic cu afișaj poate afla în timp real numărul de

telefon solicitat de postul urmărit, dar dacă nu este interesat în aceasta, sau nu are timp, pentru că au loc concomitent mai multe convorbiri, numărul telefonic solicitat se înregistrează automat pe bandă. Aceasta se realizează cu ajutorul unei frecvențe tonale. Poate credeți că, după terminarea convorbirii, odată cu plasarea pe furcă a microreceptorului, se oprește instantaneu și magnetofonul de înregistrare. Nu este chiar așa; oprirea se face, dar după un anumit timp, relativ scurt, necesar imprimării pe bandă magnetică a orei exacte la care s-a terminat convorbirea telefonică, prin racordarea automată a magnetofonului la circuitul care dă ora exactă pentru toți abonații telefonici ai unui oraș, sau prin cuplarea lui la un ceas electronic ce deservește mai multe mese pupitru.

Suntem convinși că s-a înțeles faptul că instalația de interceptare poate funcționa fără operator, toate operațiunile realizându-se automat. Prezența lui este necesară numai pentru a sesiza unele momente operative, care nu pot aștepta să fie cunoscute a doua zi, după ascultarea benzii înregistrate, precum și pentru a reduce volumul înregistrării, eliminând convorbirile neinteresante (redundante).

Apelul injurios sau cum se depistează cel ce apelează un telefon

Trebuie reținut că așa cum s-a descris anterior, pe bandă magnetică, se pare că s-au înregistrat toate datele care se pot imagina ca necesare și anume: conținutul integral al convorbirii telefonice, ora la care aceasta a avut loc, numărul de telefon apelat și deci adresa și persoana cu care a vorbit posesorul telefonului supravegheat. Si totuși lipsește o informație care, în unele situații, constituie chiar mobilul supraveglierii și anume numărul de telefon, cu alte cuvinte adresa și persoana care a apelat pe posesorul telefonului supravegheat. Aceste informații se doresc în situații când se revendică atentate sau crime politice, când se anunță în mod real sau pentru dezinformare, producerea unor evenimente, când se fac unele anunțuri deranjante, la telefoanele unor instituții publice, când se dau instrucțiuni pentru depunerea banilor în schimbul eliberării persoanelor răpite etc. Se

ştie că majoritatea centralelor telefonice automate (C.T.A.), începând cu bătrâna "Rotary", au prevăzute şi sunt echipate cu instalaţii speciale de "apel injurios", care sunt folosite de tehnicienii C.T.A. la cererea abonatului şi cu aprobările de rigoare (de obicei a Procuraturii), pentru a afla, pornind de la echipamentul de post, prin întreaga aparatură de selecţie, de comutaţie şi intercomunicaţii, postul telefonic cu care acesta este în legătură în momentul primirii apelului injurios. Operaţia trebuie făcută rapid, imediat ce s-a realizat legătura telefonică pentru că după terminarea ei nu mai poate fi identificat partenerul de convorbire, eliberându-se legătura fizică dintre cele două telefoane.

Se poate imagina, pentru că în literatura de specialitate nu se dau date, că întreaga comandă a echipamentului de apel injurios, poate fi "prelungită" până în centrul operaţional de interceptare şi să se acţioneze de acolo pentru căutarea postului chemător, dacă se doreşte păstrarea secretului, faţă de lucrătorii C.T.A. În final se afişează numărul de telefon căutat. Desigur, stimăţii cititori îşi reamintesc că au văzut operaţiuni similare în filme, atunci când trebuie să se depisteze locul de unde răpitorii transmit telefonic familiei victimei instrucţiuni de predare a sumelor de bani, în schimbul eliberării celui răpit. Necesitatea rezolvării unor astfel de situaţii apare în special în preajma şi în timpul vizitelor unor şefi de state, când foarte mulţi "binevoitori" anunţă telefonic, în special, la ambasadele statelor ai căror conducători fac vizitele respective, sau la serviciile informative ale ţărilor gazdă, care trebuie să asigure securitatea acţiunilor protocolare sau la diferite alte instituţii de presă etc., despre plasarea unor bombe, folosirea unor automobile capcană, încercări de asasinat în diferite locuri etc. Ne imaginăm uşor cât de justificată este dorinţa celor care primesc astfel de apeluri, în aceste situaţii, să discute cu aceste persoane, nu numai telefonic, pentru a lămuri, discerne şi separa ce este adevărat de ceea ce reprezintă doar imaginaţia unor minţi bolnave, iresponsabile sau pur şi simplu glume de prost gust.

Nu ştiu dacă este adevărată relatarea că, într-o astfel de ocazie, când s-a primit un telefon de acest gen, operatorul, dând dovadă de multă abilitate, a reuşit să lungească foarte mult convorbirea, să se identifice urgent locul de unde s-a apelat care, în situaţia prezentată era o apropiată cabină telefonică publică. S-a

trimis un echipaj-auto de poliție, dotat cu aparatură radio, care, ajungând la locul de destinație, a verificat prin radio, dacă mai este în funcțiune legătura telefonică. La răspuns afirmativ, ne imaginăm ușor ce a urmat. Persoana din cabină a fost invitată să relateze și să-și susțină afirmațiile pe care le făcuse telefonic. S-a reușit să se lămurească o situație și să nu trebuiască să se antreneze forțe și mijloace materiale deosebite. Sistemul de apel injurios are și limite, el nefiind eficace când apelarea se face din alt oraș sau altă țară, iar rezultatele operative sunt minime când aceste apeluri sunt foarte scurte și se fac din locuri publice, după care persoana respectivă se îndepărtează. Dacă n-ar fi fost aceste limite, poate altul ar fi fost deznodământul în cazul fostului prim-ministru al Italiei, Aldo Moro, când era necesară depistarea locurilor de unde proveneau telefoanele date organelor de stat italiene de către răpitori. Să revenim la caseta magnetică ce poartă pe ea informațiile la care m-am referit și care sunt exploatare (redate) cu ajutorul unor magnetofone profesionale. Acestea, pe lângă dotările clasice ale unui magnetofon profesional, mai trebuie să fie prevăzute cu dispozitive opto-electronice, de afișare a orei exacte și a numerelor de telefon. Redarea acestor casete se face fie de către operatorul de la masa pupitru, când există mai puțină activitate la posturile telefonice interceptate (noaptea), fie de alte persoane care rețin problemele importante, eliminând redundanța.

Se poate intercepta o națiune ?

În aceste condiții, un lucrător poate asculta 15-20 de casete, adică 20 de ore de înregistrare, în cele opt ore de activitate de redare. Un calcul simplu, ne arată că pentru o mie de posturi telefonice interceptate, care să presupunem că dau o producție zilnică de circa 1500 de casete, sunt necesari cel puțin 75 de lucrători plus 80 (20×4) operatori de la mesele pupitru care să asigure permanență în cele 24 de ore.

Deci, 155 de lucrători pentru o mie de posturi interceptate. Am prezentat acest scurt calcul, pentru a vedea cât de aberante au fost afirmațiile lui Ion Mihai Pacepa, în cartea sa "Orizonturi roșii" în care a afirmat că în România, în anul 1984, se

interceptau 3 milioane de posturi. Pe lângă faptul că în acea perioadă, după cum nici astăzi, nu avem atâtea posturi telefonice în trafic, pentru a asculta convorbirile, ar fi fost necesari peste 300 de mii de oameni. Chiar dacă socotelile ar fi exagerate și s-ar renunța și la operațiile de la mesele pupitru, rezultând numai o treime din aceștia, este firească întrebarea: ce stat, oricât de totalitar sau bogat ar fi, își poate permite luxul să plătească pentru asemenea activitate, peste o sută de mii de funcționari ? Cred că și I.M.Pacepa, autorul acestor afirmații, se rușinează acum de aberația pe care a putut-o debita.

Recent, presa ne-a prezentat date care întăresc cele afirmate până în prezent. Astfel, "Nazavisimaia Gazeta" din 8 aprilie 1993, într-un articol semnat de N.Rafenko și O.Rubinikovici, în urma unei discuții cu adjunctul șefului direcției tehnico-operative din Ministerul Securității de la Moscova, ajunge la următoarele concluzii: Deși în popor exista convingerea că fostul K.G.B., transformat în Ministerul Securității, efectuează o supraveghere totală a telefoanelor (a tuturor și de peste tot), acest control global nu poate fi posibil din punct de vedere fizic. Nu pot exista nici oameni și nici mijloace suficiente pentru aceasta. În cotidianul italian "La Repubblica" din 9 aprilie 1993 se reia această problemă și se afirmă că, pe baza datelor susținute de A.Bikov, ministrul adjunct al Securității, pe întreg teritoriul Rusiei sunt ținute sub control 2500 posturi telefonice, dintre care 1000 numai în Moscova și pentru această operație sunt folosiți circa 1300 de agenți.

Până acum am vorbit de interceptarea de tip guvernamental, denumind-o astfel pe cea executată de instituții specializate de stat, dar mai sunt și altele, după cum nici ascultarea nu se rezumă numai la convorbirile telefonice, ci se referă și la discuțiile ce se desfășoară în încăperile unde sunt instalate telefoane sau în acelea care se află în apropierea cablurilor lor. Interceptarea de tip guvernamental este foarte eficientă, atât pentru faptul că nu este necesar să se pătrundă în apartamentele unde sunt instalate posturile telefonice sau în împrejurimile acestora, cât și pentru faptul că pot fi conectate în centrale operaționale mai multe posturi, ceea ce face să scadă cheltuielile materiale și umane. După o supraveghere de circa o lună de zile a convorbirilor unui posesor de post telefonic, se pot obține foarte multe date privind obiceiurile, anturajul, relațiile,

preocupările, intențiile personale ale celui care folosește telefonul respectiv.

Interceptările telefonice neguvernamentale

Nu toți cei care se ocupă cu interceptările telefonice au "posibilitățile" și "aprobările" pe care le pot obține legal, sau prin abuz, instituțiile guvernamentale. Dintre aceștia aș aminti firmele de detectivi particulari și în special companiile industriale ai căror salariați specializați le folosesc, în scopuri de spionaj sau contraspionaj tehnico-economic, împotriva concurenței. Metodele folosite de aceștia se împart în sisteme de interceptare cu fir și radio. Din prima categorie, reținem folosirea unei bobine în care este indus câmpul magnetic produs de curentul electric modulat și care la rândul lui reproduce semnalele audio ale microfoanelor (fig. 2).

Cuplarea dintre bobină și cablu, sau aparatul telefonic, trebuie făcută "cât mai strâns" (foarte apropiate), pentru ca nivelul de tensiune indus în bobină să fie suficient de mare, astfel ca, după amplificare și înregistrare, convorbirea să poată fi inteligibilă, utilizabilă.

Metoda descrisă este foarte greu de implementat, în special datorită faptului că rezultatele obținute sunt, în final, submediocre. Mai răspândită este metoda branșării cu ajutorul unei rețele de adaptare (care trebuie să conțină cel puțin un condensator) a dispozitivelor de interceptare (amplificator, magnetofon, cască) direct pe perechea de fire care leagă telefonul supravegheat cu C.T.A. Această branșare se face fie în același loc în dispozitivul anexă al telefonului (rozetă) unde cablul se leagă cu cordonul aparatului telefonic, fie cel mai adesea în spatele cutiei terminale (terminal-box) care de regulă sunt plasate în subsolul clădirii, în casa scării, sau pe clădiri și stâlpi telefonici. Cuplarea trebuie făcută în așa fel, încât să nu modifice tensiunea existentă pe linia telefonică, să nu deformeze curentul, să nu perturbe buna funcționare a C.T.A. sau a telefonului urmărit și să nu poată fi sesizată, prin măsurători simple de către tehnicienii companiei de telefoane. În orice caz, recomandăm "curioșilor" să nu încerce să cupleze direct pe linia telefonică o cască sau un magnetofon

deoarece vor avea surprize neplăcute, printre care și deteriorarea lor.

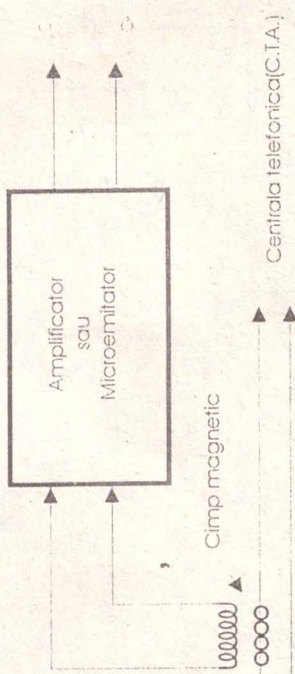
Aceste sisteme de interceptare, pe lângă unele avantaje, prezintă și serioase greutăți legate de faptul că branșarea trebuie prelungită până la punctul unde se organizează ascultarea sau înregistrarea. Sigur, se pot găsi soluții care depind foarte mult de condițiile locale dar este cert că nu este o treabă ușoară. De aceea, multe companii de detectivi particulari recurg la folosirea, în acest scop, a unor metode "fără fir" sau sisteme radio, prin folosirea unor microemitoare care rezolvă (foarte ușor) legătura dintre locul de interconectare, unde se captează convorbirea și punctul de ascultare sau cel intermediar (fig. 3)

Modul cum va fi plasat acest microemitor depinde de ingeniozitatea celor care realizează această operație, fie în aparatul de telefon propriu-zis, fie oriunde de-a lungul cablului telefonic, cel mai probabil în așa-numitele cutii terminale unde mai multe perechi de fire se unesc pentru a forma un cablu multifilar care se prelungește până la C.T.A. Alimentarea cu energie a acestor microemitoare se realizează fie din baterii încorporate, când este vorba de o interceptare de scurtă durată, fie din tensiunea electrică cu care C.T.A. alimentează fiecare telefon. Acest microemitor are fie microfon propriu când se interceptează convorbirile din jurul telefonului, fie își ia "semnalul" din curentul modulat ce circulă în linia și aparatul telefonic. În cel de-al doilea caz, deși se asigură o calitate mai slabă a audiției, se obține o disponibilitate mai mare la plasarea acestora.

Din punct de vedere al alimentării și a modului cum sunt montate aceste dispozitive, se rețin două metode și anume: în serie, pe un singur fir al perechii telefonice sau paralel când branșarea se face pe ambele fire.

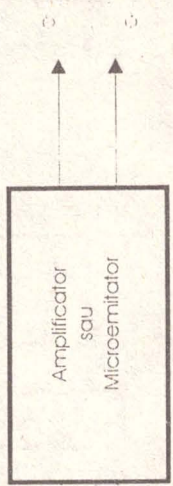
Foarte uzitată este mascarea microemitorului în carcasa microfonului telefonului, astfel că aici se găsește atât microfonul cărbune cât și microemitorul. Facem din nou apel la memoria peliculei pentru a reaminti cititorului multe scene din filme, în care se vede cum se intră într-un apartament, se ridică microreceptorul telefonului din furcă, se deșurubează învelișul protector din bachelită sau plastic, se scoate microfonul și se înlocuiește cu altul, identic ca formă, dar care are în plus și un microemitor care transmite conținutul convorbirilor până la 100-200 metri, unde se află un receptor. Firmele producătoare au anunțat și

Punct de receptie



Punct de receptie

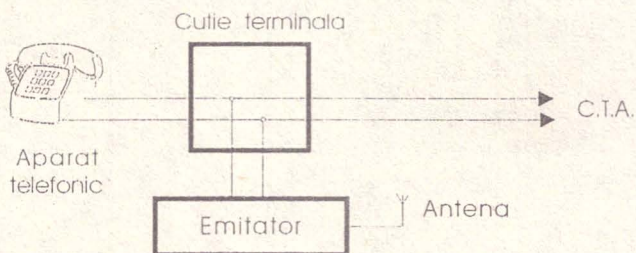
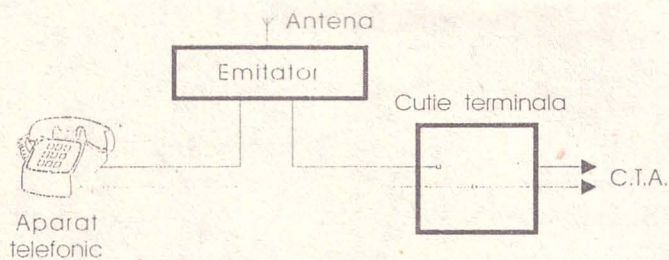
Bobina de inductie



Bobina de inductie

Fig. 2 Interceptare telefonica prin inductie

EMITATOARE PE LINIA TELEFONICA



EMITATOR IN TELEFON

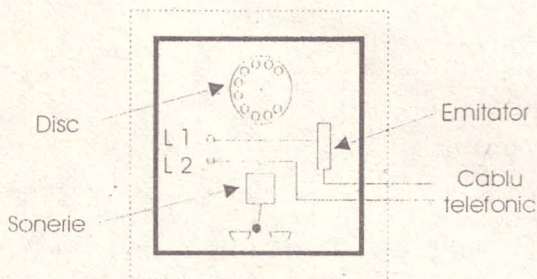
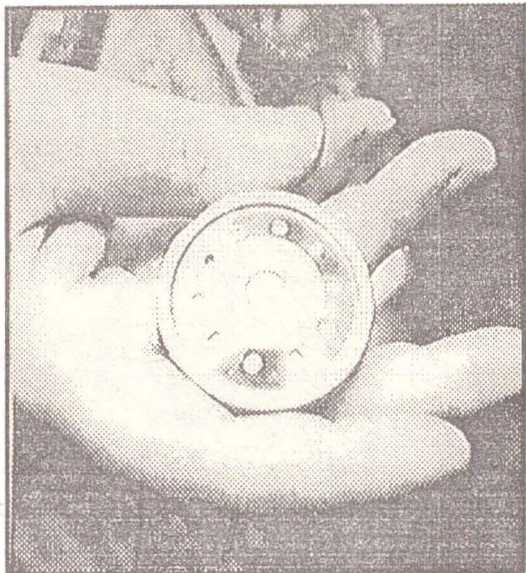
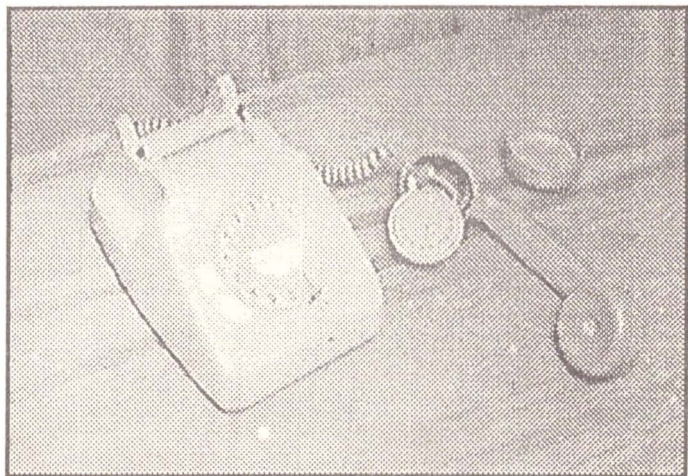


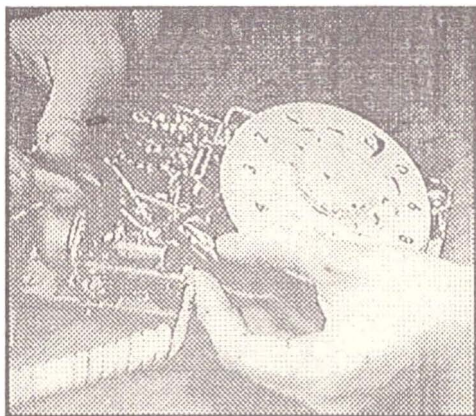
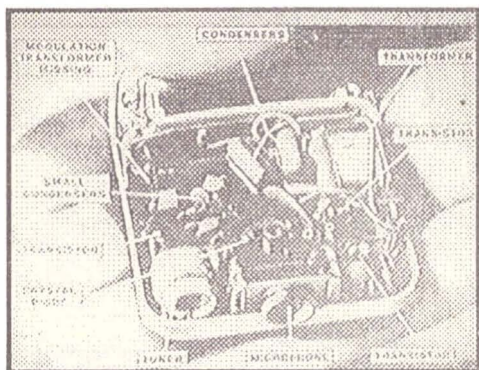
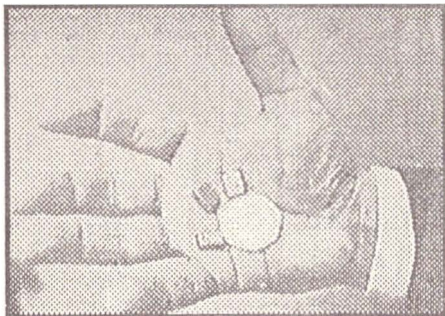
Fig. 3 Instalari de emitatoare pentru interceptari telefonice



Emitator montat in microfonul aparatului



Montarea emitatorului in microreceptorul aparatului



Montarea dispozitivelor de interceptare în aparatul de telefon.

prezentat microemițătoare destul de mici ca dimensiuni, în așa fel încât să poată fi mascate sau ascunse în foarte multe piese componente ale telefonului. Modulația folosită este de tip FM (modulație de frecvență), dar s-au construit și microemițătoare cu tipuri de modulație mult mai sofisticate, pentru a îngreuna detectarea interceptării respective și localizarea emițătorului, dar despre acestea vom vorbi ulterior.

Stabilirea puterii microemițătorului folosit, caracteristică care determină în cea mai mare parte, distanța până la care acesta poate fi recepționat, se stabilește în urma unui compromis între dorința ca raza de acțiune (bătaia) să fie cât mai mare și necesitatea ca acesta să nu fie recepționat accidental sau de către echipe specializate. Frecvența emițătorului este, în prezent, în jur de 120 MHz, pentru a fi mai mare ca frecvența maximă a receptoarelor obișnuite, din comerț, care au banda UKW (88-108MHz), încât să nu poată fi ascultat cu acestea.

Ascultarea telefoanelor moderne - o problemă facilitată

Pentru a ușura munca celor care se ocupă de interceptarea telefoanelor, constructorii acestor aparate au fabricat și în ultimul timp s-au răspândit foarte mult, posturi telefonice care, pentru a da posibilitatea să se recepționeze apelul telefonic de la distanțe mai mari și pentru a putea realiza convorbiri telefonice dintr-un apartament, dintr-o rezidență, din curtea imobilului și nu numai din locul unde este instalat telefonul (prelungirea facilităților telefonului la o distanță de 100-200 m), au fost împărțite în două părți constructive. Prima parte este o microcentrală fixă care realizează legătura cu C.T.A., iar a doua este cea formată din microreceptorul portabil cu antenă care, pe lângă microfon și receptor, posedă și dispozitivul de formare a numerelor. Între aceste două părți există o legătură radio-duplex în limitele prezentate mai sus prin emițătoarele-receptoarele existente în cele două părți ale telefonului. Deci, obținând facilitarea de a putea vorbi la telefon de pe marginea piscinei, de la bucătărie, de pe peluza din fața casei, practic s-a renunțat la asigurarea secretului convorbirii care poate fi ascultată de oricine

care dispune de un receptor adecvat, pe o rază de 200 de metri, fără să se mai obosească să plaseze un microemițător. Trebuie spus însă că, de curând s-au construit aparate telefonice de acest tip cărora, pentru a îngreuna interceptarea, în legătura radio dintre cele două părți li s-au introdus semnale de recunoaștere.

Plastic și sugestiv, avantajele și deficiențele acestui tip de telefon sunt redată în filmul american "O crimă mică și perfectă", producție 1992. O tânără familie americană, care avea un copil de câteva luni se mută într-o casă nouă, cu mai multe încăperi, la periferia orașului. Pentru a supraveghea de la distanță activitatea copilului, tatăl acestuia a cumpărat două păpuși speciale, de fabricație japoneză. Într-una era montat un microemițător (baby-monitor) care se plasa în camera copilului iar în cealaltă un receptor și se punea, după nevoie, în apropierea locului unde se aflau părinții. Astfel, aceștia puteau ști când plânge, țipă sau doarme copilul. Frecvența de lucru a acestui sistem de monitorizare era aceeași ca a unui telefon cu "antena" din vecinătatea casei. Astfel, mama copilului, supraveghind păpușa cu receptor, a interceptat fără să vrea convorbiri telefonice prin care se punea la cale o crimă pasională. Pentru scopul lucrării nu este interesant cum au fost identificați și arestați criminalii, dar este important de reținut că aceste telefoane sunt vulnerabile, convorbirile prin acestea au putut fi interceptate și accidental, fără să mai vorbim de cazurile voite. Dacă pentru supravegherea unui bebeluș, microemițătoarele și receptoarele se maschează în păpuși, se găsesc în mod sigur obiecte în care să se monteze aceleași emițătoare-receptoare când este vorba de monitorizarea soției, secretarei, a unui partener sau concurent de afaceri.

Pentru a se crea o imagine completă a modului cum funcționează o legătură telefonică la distanță mare și a se deduce de aici marile posibilități de interceptare, se redă în continuare, selectiv, din articolul "Despre dispariția lentă a secretului comunicării" de H.H. Pardey și N.Schiffhauer din suplimentul "Technick und Motor" al cotidianului german "Frankfurter Allgemeine Zeitung" din august 1992:

"Cu cât confortul de a telefona se impune mai mult în viața cotidiană, de la o piscină, din autoturism, de la berărie sau de pe vasul de agrement, cu cât convorbirile se desfășoară mai intens nu prin cablu ci prin unde radio cu atât crește mai puternic riscul interceptării."

"Ceea ce reprezintă o acțiune a statului reglementată juridic și necesită pentru interceptarea unei legături un minim de know-how profesional devine, prin modificările tehnice - și în curând prin cele juridice - la îndemâna fiecărui cetățean. În comerț se găsește de puțin timp o paletă largă de receptoare radio care pot intercepta și emisiuni dincolo de limitele admise ale spectrului de frecvențe uzuale. Ele se numesc receptoare de bandă largă sau scannere și se găsesc într-o gamă largă de modele, începând cu cele portabile până la cele integrate în aparatele de radio de pe mașini și în sistemele muzicale Hi-Fi."

"Până în prezent, deținerea și folosirea unor asemenea aparate în Germania sunt interzise. O excepție o constituie radioamatorii autorizați care pot deține și folosi astfel de aparate atâta timp cât acestea - și aceasta este regula - permit și recepția frecvențelor folosite de radioamatori. Interceptarea frecvențelor nepermise și folosirea informațiilor rezultate sunt, de asemenea, interzise și pasibile de pedeapsă atât pentru radioamatori cât și pentru cetățenii obișnuiți".

"În această privință nu se va schimba nimic chiar dacă, în viitorul apropiat se va permite deținerea de receptoare cu bandă largă. Acest pas va fi întreprins în așa fel încât nu vor mai exista limite de ascultare a frecvențelor. Însă, ca și până acum, va fi necesară, pe lângă aprobarea germană sau a unei țări europene de funcționare a aparatului și înștiințarea Serviciului Federal de Poștă și Telecomunicații. Condiția este ca receptorul să cuprindă și frecvențele radio uzuale".

"Chiar dacă deținerea scannerului este (încă) interzisă, nimeni nu a fost oprit să încalce secretul convorbirilor telefonice. Participanților la traficul radio pe multe frecvențe le este clar faptul că sunt controlați periodic și se comportă ca atare. Pe de altă parte, legea a fost aplicată diferențiat: unii clienți nevinovați ai comerțului prin case de comenzi, după primirea aparaturii radio interzise, au fost vizitați repetat de către poliție, în timp ce, în anumite domenii scannerul a devenit un instrument folosit în mod curent și nu deranjează pe nimeni, cu condiția să nu se facă prea mare tapaj. Această permisiune elimină echivocul generat de reglementările îndoielnice și practica supravegherii, dându-se câmp liber unui alt drept fundamental: accesul liber la sursele de informare".

"Pe de altă parte, interdicția îi va împiedica pe cei care

interceptează ocazional, convorbiri, să afle cu cine vorbește fiica la radio-telefon și despre ce".

"Pe viitor, va trebui să se ia mai frecvent în calcul posibilitatea de interceptare, mai ales în cazul divorțurilor și a certurilor cu vecinii, nemaiținându-se seama de faptul că infractorii care-ți golesc casa pe perioada concediului dispun de mult timp de asemenea aparatură. Nu este însă cazul să intrăm în panică și să credem că în curând ne vom spiona reciproc. Trebuie să avem în vedere riscurile impuse de facilitățile create de telefonía modernă".

"Motivația pentru care Ministerul Federal al Poștelor și Telecomunicațiilor armonizează liberalizarea reglementărilor germane cu dreptul european mai are o componentă care nu trebuie subapreciată: dacă se mărește riscul interceptării, crește și nevoia de protecție; industria dispune deja de aparatura corespunzătoare care să fie pusă la dispoziția clienților, la prețuri competitive.

"Fiecare organizație sau persoană care comunică printr-un sistem nesecretizat, trebuie să fie conștientă că poate fi interceptată de un terț." Acest avertisment nu este tipărit cu minuscule în instrucțiunile companiei Telecom, ci este întâlnit în raportul pe 1990 al Oficiului pentru Apărarea Constituției care permite formarea unei idei despre interceptarea tehnică profesionistă. Folosind mijloace tehnice cu șapte ani mai vechi decât cele din Occident, organele din R.D.G. supravegheau automat traficul radio din rețeaua telefonică a Republicii Federale. Se înregistrau convorbirile dintre anumite posturi telefonice interesante din punct de vedere politic și economic. Stațiile de interceptare cu nume codificate ca: "Cormoran", "Lupine" sau "Rubin" au trecut, ca și rețeaua armatei sovietice din fosta R.D.G., în posesia serviciilor corespunzătoare din vechile landuri federale. Că desființarea Ministerului pentru Securitatea Statului nu a modificat deloc pericolul interceptării, se vede și din raportul OFAC. Însă, acest raport trece sub tăcere din partea cui survine astăzi încălcarea secretului convorbirilor telefonice, poate și pentru faptul că B.N.D. (Serviciul Federal de Informații) și Biroul Federal pentru Statistica Telecomunicațiilor sunt la ele acasă și cooperează cu servicii străine, cum ar fi N.S.A. (Agenția Națională de Securitate din S.U.A.). Prin dezvoltarea comunicațiilor radio s-au mărit și posibilitățile de interceptare particulară a convorbirilor

private și a transmisiilor prin telefon".

"Interlocutorul care vrea și poate vorbi din grădina sa, spre exemplu, cu primarul Brian Young din Insula Pitcairn din Pacific nu sesizează dedesubtul acestei rețele. Stând în hamac și spunându-i: "Bună dimineața, Brian, ce mai faci ?", el intră într-o rețea vastă cu această insulă de numai 4,6 km²: telefonul fără fir emite pe frecvența de 900 MHz (rază de acțiune 300 m), este recepționat de telefonul mobil care îl transferă într-o rețea pe frecvența de 450 MHz (rază de acțiune - mai mulți km) de unde este transferat la stația de bază a Poștei. În loc să folosească cablurile sau fibrele de sticlă, Poșta transmite prin releu în frecvențele de la 1,7 la 30 GHz convorbirea la centrul de transmisii prin satelit de la Usingen (Germania). Transmisia între Pământ și satelit are loc pe frecvențele de la 12 la 14 GHz."

"Poșta neo-zeelandeză primește acest semnal din satelit și îl transmite mai departe printr-un releu, în cazul nostru printr-un emițător pe unde scurte care, pe frecvența de 18 MHz, ajunge în Pitcairn. Acolo operatorul radio transmite convorbirea lui Brian Young."

"Posibilitățile de interceptare a acestei convorbiri sunt nenumărate. Telefonul fără fir și telefonul mobil pot fi interceptate fără probleme cu scannere, acele aparate de radio care au un domeniu larg de frecvență și a căror funcționare este deocamdată interzisă în Germania. Interceptarea releelor, datorită frecvențelor înalte și sistemelor complicate de codificare, este accesibilă numai organelor de stat; astfel au fost interceptate de STASI convorbirile telefonice între Berlin și Usingen pe frecvența de 20-30 GHz. Dificultăți asemănătoare de natură tehnică se întâlnesc și la interceptarea convorbirilor prin satelit însă, datorită rețelei mondiale, crește numărul celor ce pot face interceptarea. Ultima parte a traseului poate fi ascultată de orice persoană care are un aparat bun pe unde ultrascurte".

"Interceptarea convorbirilor prin releu reprezenta 35% din activitatea lucrătorilor STASI care se ocupau de interceptarea convorbirilor telefonice la mare distanță; alte 25% reprezentau interceptarea convorbirilor efectuate din autoturisme."

"Interceptarea convorbirilor, a cărei dimensiune rămâne necunoscută, este la îndemâna oricui, mai ales dacă partenerii comunică direct prin releu. Poliția, pompierii și serviciile de salvare au rețele radio ample, prin care informațiile confidențiale sunt

rareori codificate pentru a fi protejate de interceptare neautorizată".

"Nu numai aceste 'Organe și organizații cu sarcini de securitate' (B.O.S.) folosesc eterul în activitatea lor, ci și medicii, întreprinderile de expediție, căile ferate, piloții, societățile de pază ca și vânătorii. Ei folosesc frecvențele care sunt alocate pentru 'comunicații mobile nepublice'. Lor le sunt repartizate canale de emisie anume stabilite."

"Persoanele și frecvențele folosite sunt trecute în 'Manualul utilizatorului pentru UUS', apărut în editura 'Siebel'. Utilizatorul realizează pentru prima dată cât de vulnerabil este secretul convorbirilor telefonice. Dacă se mai adaugă și posibilitățile scannerului, nu mai există nici un mijloc de apărare."

Se apreciază că în Germania există în proprietate particulară 400000 de scannere. Liberalizarea deținerii, motivată de Ministerul Poștelor și Telecomunicațiilor prin comerțul liber din cadrul Comunității Europene nu va mări pericolul unei interceptări organizate; cine vrea să folosească informații obținute pe această cale, nu a fost nici până acum împiedicat de interdicția de deținere a aparaturii. Ca și până acum secretul convorbirilor va fi apărat de interdicția interceptărilor, însă o securitate cu adevărat eficientă nu o poate oferi decât o securitate inteligentă".

*

* *

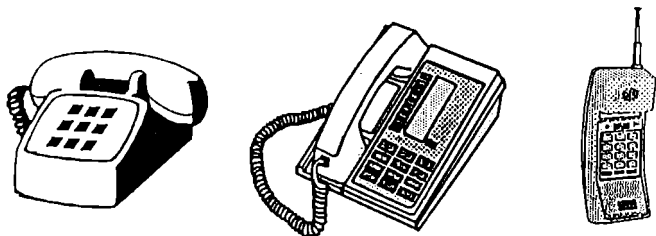
Se vor găsi unele persoane care, poate, vor considera că cele afirmate n-au acoperire juridică, pentru că legile (Constituția, Codul Penal etc.) țărilor democratice interzic astfel de activități de interceptare a convorbirilor. Nu se dorește intrarea în polemică cu dâșii, dar de ce atunci o întreagă industrie produce o gamă foarte variată de aparatură și dispozitive destinate rezolvării tuturor problemelor tehnico-operative pe care le ridică spionajul sau contraspionajul, inclusiv ascultările secrete ?

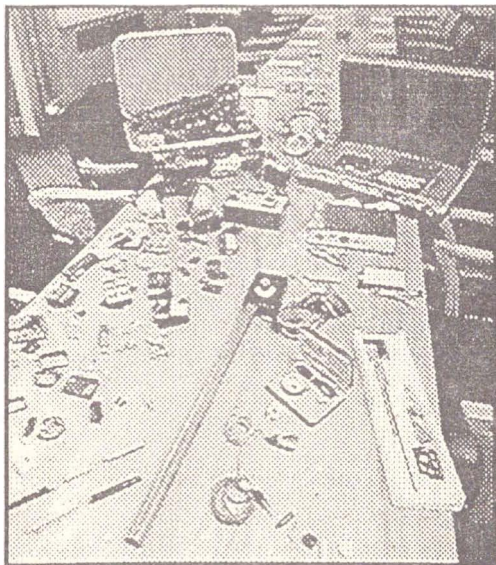
De ce, încă din 1972, peste 250 de companii numai în Anglia prosperau, ocupându-se cu aceste afaceri ? De ce se găsesc în Germania și Austria mii de magazine care

comercializează astfel de produse ? De ce s-au editat cataloage în care sunt descrise, cu lux de amănunte, performanțele fiecărui aparat sau dispozitiv ? De ce se organizează cu regularitate expoziții și conferințe internaționale pe tema așa-zisei aparaturi de poliție, de apărare, antiteroristă etc. care, în fond, epuizează întreaga gamă de aparatură ofensivă și defensivă și care poate fi vândută publicului larg ? De ce firme foarte serioase din Occident vindeau țărilor din Est, în special în anii '80, chiar ocolind embargoul, aparatură sofisticată - ultimul tip de laser pentru ascultări - sau aparatură de observat și fotografiat cu amplificator de lumină din generația a treia cu ajutorul căreia se poate vedea și fotografia la lumina unei stele sau la cea emisă de un chibrit aprins. (Se cunosc rezultatele deosebite obținute de această armă în războiul anglo-argentinian din Insulele Falkland-Malvine și cel recent, din Golf).

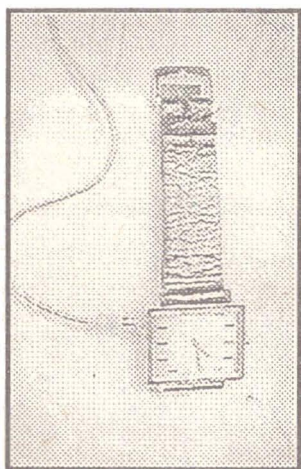
În lucrarea "*The business of Spying*", de Brian Murphy se dau foarte multe date referitoare la firmele care produc aparatură de spionaj-contraespionaj, în special de interceptare telefonică, produsele acestora și principalele lor caracteristici.

Din presa franceză reținem că France Telecom îi sfătuiește pe șefii de întreprinderi să se doteze cu un "post al directorului" care are o funcțiune pudic botezată de către producător "intervenție discretă". Este vorba despre o posibilitate de ascultare silențioasă, care le permite să se brânzeze oricând pe postul telefonic al oricărui funcționar de-al lor funcție care este integrată în autocomutatorul întreprinderii. Foarte în vogă în marile societăți care produc materiale strategice, pentru a verifica dacă inginerii nu sunt cumva vânduți inamicului, această practică are tendința de a se răspândi.





Camera de prezentare a unei companii care produce
si comercializeaza dispozitive de interceptare



Microfon mascat intr-un ceas de mana

CAPITOLUL IV

NE CUNOAȘTEM OARE TELEFONUL ?

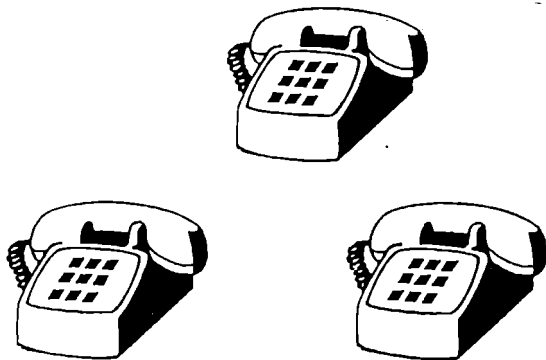
Se poate critica faptul că s-a abordat problema interceptării convorbirilor telefonice fără a se da un minim de date tehnice, privind organizarea și funcționarea C.T.A., precum și a aparatului de telefon. Pentru a înțelege modul cum se pot intercepta convorbirile, care se poartă nu numai prin telefoane, ci și în camere în apropierea acestora sau în încăperi străbătute de cablurile telefonice, este necesar să prezentăm succint aceste informații. O centrală telefonică automată pe care am numit-o C.T.A. este o unitate, dintr-un vast sistem electronic de telecomunicații care deservește de regulă 10 mii de abonați. Ea are următoarele părți componente principale: repartitorul (unde se termină cablurile care leagă posturile telefonice cu C.T.A. și de unde se pleacă spre echipamentul de linie al centralei) și aparatura de comutație automată. Aceasta din urmă, odată cu dezvoltarea tehnicii, a evoluat de la selectoare, relee, la dispozitive complet electronice și va putea conecta un telefon cu altul din cadrul aceleiași centrale sau, prin cablurile de intercomunicații, cu un telefon dintr-o altă C.T.A. (după dorința solicitantului).

Pe lângă aceste părți principale, C.T.A. mai dispune de o sursă de tensiune de curent continuu cu care sunt alimentate permanent posturile telefonice, generatoare sau mașini de ton, de apel, precum și pentru a semnaliza că postul solicitat este ocupat (ton de ocupat). Trebuie lămurite aceste probleme pentru că, o parte din facilitățile și limitele acestora, sunt folosite pentru a întreține aparatura de interceptare. Astfel, multe din dispozitivele de captare a convorbirilor sunt alimentate chiar din sursa de energie electrică, care este folosită și pentru posturile telefonice. Telefonul standard, folosit de foarte mulți, dar cunoscut în detaliu de foarte puțini, posedă în primul rând un microfon, plasat în micreceptor, în partea în care acesta se leagă cu un cordon de restul aparatului și care transformă undele sonore (vocea celui care vorbește) în semnale electrice. Este în general, un microfon

cu cărbune, descoperit în 1876 de Graham Bell, ce funcționează numai când este alimentat în curent continuu și care sub influența undelor sonore, schimbându-și rezistența, modulează curentul electric care-l străbate.

La celălalt capăt al microreceptorului se află montată casca magnetică ce transformă variațiile curentului din bobina sa în unde sonore, cu ajutorul diafragmei sensibile. O altă piesă importantă a telefonului este discul (sau claviatura cu memorie) cu ajutorul căruia se formează numerele de telefon dorite. Astfel, dacă dorim să transmitem o cifră a numărului de telefon dorit, după ce am rotit discul de la cifra respectivă, în sensul rotirii acelor unui ceasornic, până la capăt, la revenirea acestuia se întrerupe de tot atâtea ori curentul în linie rezultând astfel numărul de impulsuri care vor acționa în echipamentul de selecție.

Așa cum rezultă din literatura de specialitate, componenta care a dat cea mai mare bătaie de cap celor care se ocupă de interceptări este întrerupătorul, acționat de furca pe care se așează microreceptorul. Când acesta este așezat în poziția de repaus, întrerupătorul este deschis, neexistând legătura fizică între microfon, cască și linia telefonică. În aceste condiții, la bornele liniei telefonului se poate măsura o tensiune de 48 V și nu circulă nici un curent electric. Când se pune în funcțiune telefonul prin ridicarea microreceptorului, un resort împinge furca închizându-se contactul întrerupătorului, se realizează astfel legătura fizică între componentele telefonului și linia telefonică, tensiunea scăzând la 12 V și rezultând un curent de circa 40 mA care circulă prin microfonul cu cărbune. O ultimă piesă pe care doar o amintim este soneria, care, primind trenul de apel alertează pe posesorul telefonului că este solicitat (fig. 4).



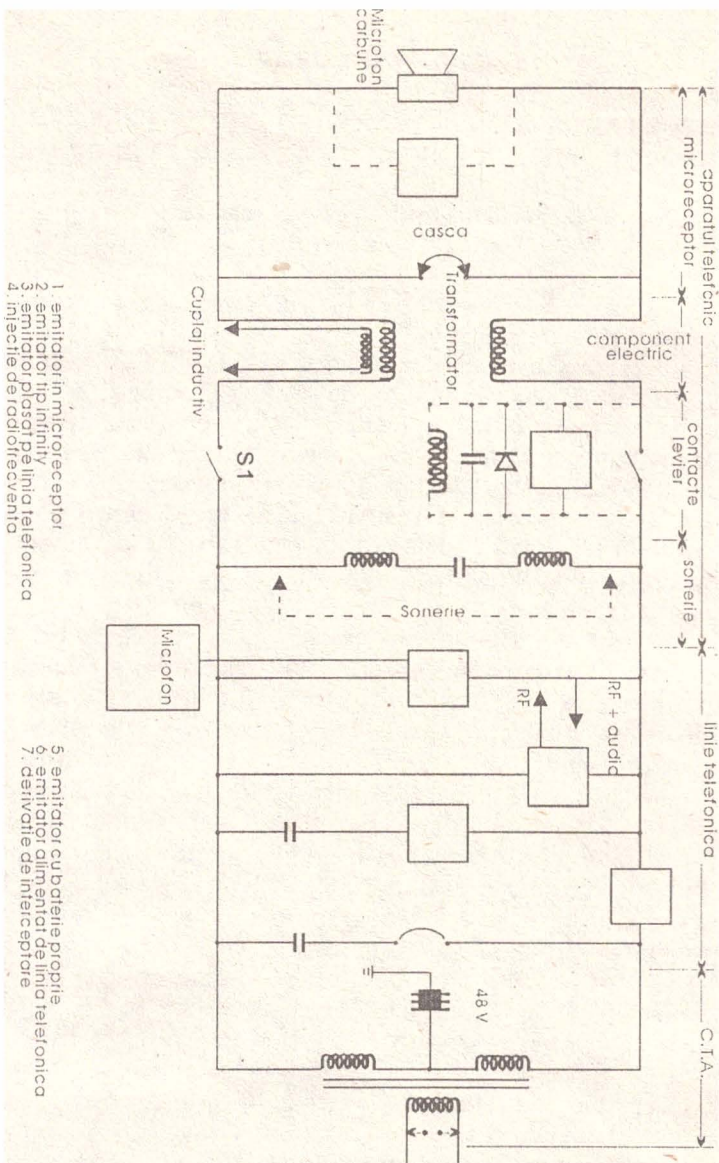


Fig. 4. Schita sinoptica a interceptarii telefonice

ASCULTAREA CONVORBIRILOR INTERIOARE CU AJUTORUL TELEFOANELOR ȘI CIRCUITELOR LOR

**Dispozitivul antifurt este în realitate
un aparat de ascultare**

Una din metodele care rezolvă acest tip de interceptare a discuțiilor și, corespunzător acestuia, și dispozitivul specific, căruia în presa și cataloagele de specialitate i s-au făcut cea mai mare reclamă, poartă numele de "Infinity transmitter" sau "Harmonica bug", dificil de tradus în limba română în termenii "transmițător infinit" sau "muzicuță parazită" (ploșniță). Este bine să spunem că principalele date prezentate în acest capitol dar și în altele ce urmează, au fost inspirate și verificate cu cele furnizate în lucrarea de uz intern, publicată în S.U.A., de către Telecommunication Publishing Inc. intitulată "Protecting your privacy" - A comprehensive Report on Eavesdropping Techniques and Devices and their Corresponding Countermeasures, în traducere: "Protejarea secretelor" - un studiu despre tehnici și dispozitive de ascultare și măsuri corespunzătoare de contracarare, o lucrare completă care descrie, în mod obiectiv, analizează și apreciază toate mijloacele de interceptare folosite pe plan mondial. Dar să revenim la problema tratată și să spunem că termenul "infinit" a fost dat, datorită pretenției firmelor constructoare, că interceptarea convorbirilor cu ajutorul acestei metode se face de la o distanță "infinită" (practic de la un oraș la altul, sau de la o țară la alta). În fond, acesta nu este un transmițător fără fir, ci un amplificator cu microfon, care se cuplează (activează) pe linia telefonică printr-un comutator, comandat de un ton vocal. Acest dispozitiv se plasează în secret, în camera în care se dorește ascultarea convorbirilor care se poartă, fie chiar în interiorul telefonului sau, poate, pe linia telefonică, dacă aceasta străbate încăperea respectivă, sau trece prin apropierea ei. Cel care realizează ascultarea, pe lângă dispozitivele clasice de ascultare și înregistrare, mai trebuie să posede o "muzicuță" care emite un semnal de 440 Hz. De aici și a doua denumire a dispozitivului.

Modul de întrebuințare, descris în prospectele comerciale și instrucțiunile folosite, arată că persoana care realizează interceptarea respectivă formează numărul de telefon urmărit și, înainte ca mașina de apel din C.T.A. să trimită "trenul" de apel și abonatul să răspundă, în fața microfonului telefonului suflă în muzicuța respectivă și astfel tonul, sau mai concret spus semnalul electric, ajunge până la telefonul urmărit, conectându-se în linie dispozitivul de ascultare.

Odată acesta branșat, se produce un anumit consum pe linia telefonică și, implicit, o anumită scădere a tensiunii continue de la bornele telefonului, ceea ce "simulează" ridicarea microreceptorului și din această cauză apelul se oprește. Dacă la primele încercări de interceptare, apelul totuși ajunge, soneria telefonului este activată și cel urmărit răspunde, se înțelege că se motivează față de acesta că s-a format un număr greșit iar când interlocutorul pune telefonul pe furcă, se folosește din nou muzicuța, pentru activare.

Când din ascultarea convorbirilor rezultă intenția celui interceptat de a folosi propriul telefon, pentru a-i se permite acest lucru, cel ce realizează ascultarea își închide propriul telefon și astfel se decuplează dispozitivul de interceptare. În aceste condiții, aparatul de telefon ascultat este apt de funcționare, poate primi apel și forma numere. Din sumara descriere, rezultă că această metodă este bine să fie folosită numai pentru ascultări de scurtă durată, în momentele operative când se cunoaște că într-o încăpere se poartă discuții importante. Pentru a nu avea probleme de încălcare a prevederilor legale, atunci când aceste dispozitive sunt oferite spre vânzare publicului larg, li se face reclamă ca aparatură foarte ieftină pentru paza propriilor locuințe. Chipurile, o persoană care dorește să-și apere casa, montează astfel de dispozitive, în principalele încăperi ale apartamentului și de oriunde s-ar afla, activează dispozitivul formând propriul său număr de telefon, iar după folosirea muzicuței poate asculta dacă în cameră se află vreun spărgător !

Oare este dificil ca cel care cumpără să-și imagineze că procedând exact în același mod, poate să-și asculte și soția, sau pe oricine, în al cărui telefon a avut posibilitatea să monteze un astfel de dispozitiv "infinity" ?

Succesul în folosirea acestei metode, depinde de modul cum funcționează diferitele sisteme din centralele telefonice prin

care se realizează legătura între cele două telefoane și anume dacă această conectare, nu fizică, dar realizată pentru semnale electronice, de audiofrecvență, se face înaintea primirii "trenului" de apel, pentru ca telefonul supravegheat să poată primi semnalul provocat de muzicuța la care ne-am referit și să branșeze sistemul "infinity".

Din datele cunoscute, acest dispozitiv se folosește în special în S.U.A. și Israel unde centralele telefonice permit, în condiții bune, utilizarea sa.

Sistemul de ascultare descris are, pe lângă unele performanțe și multe limite printre care, cea mai importantă se referă la faptul că este necesar, sub o anumită formă, să se pătrundă în apartamentul persoanei care urmează să fie ascultată, pentru a se instala dispozitivul. Un alt dezavantaj, destul de mare care face ca această metodă să nu poată fi folosită pentru lungă durată, rezultă din faptul că circuitul telefonic, în momentele în care se face interceptarea se "prezintă" față de centrala telefonică căreia îi aparține și față de cei ce-l apelează ca fiind mereu în convorbire (ca un post "ocupat").

Dispozitivele speciale aparținând centralei telefonice, de regulă "aruncă" afară astfel de posturi, sau alertează într-un anumit mod compania de telefoane ai căror tehnicieni, prin măsurarea tensiunii la bornele aparatului, pot determina foarte ușor prezența unui dispozitiv de ascultare. Sunt însă sisteme, metode și dispozitive, mai "pământene" și mai eficiente, dar nu la îndemâna tuturor.

Organizarea și folosirea interceptărilor de către instituțiile guvernamentale specializate

Atunci când am prezentat câteva date despre aparatul telefonic am anticipat că "bătălia", dacă se poate numi așa, dintre cei ce se ocupă cu interceptările (servicii specializate guvernamentale sau particulare) și companiile de telefoane se va da în jurul modului de funcționare al întrerupătorului (contactului) care este comandat de furca telefonului.

Primii doresc ca acesta să fie închis în perioadele când telefonul nu funcționează și microreceptorul este pe furcă, având astfel acces, când doresc, până la microfonul și casca telefonului interceptat. Companiile de telefon au interesul ca acesta să fie

închis numai în perioadele când aparatul telefonic este întrebuințat și consumă 40 mA. Societățile de telefoane și-au proiectat, în acest sens, atât aparatura de abonat cât și sistemele telefonice ale C.T.A.

Din această "luptă" a rezultat, ca în multe alte situații similare, un compromis, prin care să nu se deranjeze nici funcționarea C.T.A. și nici a telefonului, dar să rezulte și posibilitatea activării microfonului cu cărbune și a transducerii semnalului rezultat de la acesta până la locul de ascultare. Dispozitivele care realizează aceste deziderate poartă în literatura de specialitate din limba engleză și în lucrarea la care ne-am referit denumirile de "listen-backs" și "keep alives". Traducerea, în limba română, deși nu exprimă exact sensul din limba engleză, poate fi "a asculta în spate (înapoi) și a "ține în viață". Pentru a înțelege primul termen, nu e lipsit de interes să-l asociem cu titlul cunoscutului film american "In spatele ușilor închise". Desigur, nu este vorba de a închide contactul întrerupătorului sau de un scurt circuit brutal cu o bucată de sârmă pentru a realiza o continuitate fizică, ci se are în vedere să se asigure o anumită continuitate electrică, fie în curent continuu fie alternativ, după "solicitările" dispozitivului de interceptare.

Sunt mai multe posibilități de a obține "ocolirea" contactului deschis al întrerupătorului, dar toate trebuie să urmărească alimentarea microfonului cu cărbune sau a altui dispozitiv de ascultare și în același timp, curentul electric să nu fie mai mare de 8-10 mA, deoarece la o valoare superioară (peste 10mA) C.T.A. acționează ca și cum telefonul este în funcțiune, trimițând spre acesta tonul de apel.

O soluție concretă care a rezolvat practic aceasta problemă și în România, a fost descrisă după cum rezultă din arhivele publicate, după o declarație a fostului colonel de securitate Golumbovici. Audiut în cazul Pătrășcanu el a arătat că, încă din 1948 în Ministerul de Interne din România se folosea ascultarea interioară a unor încăperi, cu ajutorul unor telefoane modificate, folosind datele puse la dispoziție de un tehnician specialist în comunicații, pe nume "Smelas" (nu se știe dacă era un nume real sau conspirativ). Pentru date suplimentare se prezintă anexa a IV-a, "Ziariștii și sursele lor abordează problema tehnicii de interceptare", după un articol cu același titlu din ziarul "Universul" din 25-26 februarie 1993.

Fără a se da și detalii tehnice, se poate însă ușor imagina că nu putea fi vorba în acei ani, în România, când nu apăruse tranzistorul (s-a inventat în 1949, la laboratoarele Bell Telephone), decât de șuntarea, în mod secret, a contactului din telefon cu o rezistență și un condensator care pentru curentul alternativ de frecvență vocală, să reprezinte doar câțiva ohmi. Astfel, se obține un curent continuu de câțiva miliamperi care va activa la limita de jos a funcționării microfonul cu cărbune (se reamintește termenul de a "ține în viață") și centrala telefonică nu va sesiza automat acest consum, decât, bineînțeles, cu măsuri și măsurători speciale.

Semnalul electric de audiofrecvență și așa destul de mic, datorită slabei alimentări a microfonului cu cărbune (de 5-6 ori mai mică ca cea normală) nu va întâmpina decât impedanța liniei telefonice, deoarece rezistența adăugată este șuntată în curent alternativ, așa cum s-a arătat. S-au obținut, în acest mod, rezultate mulțumitoare pentru acele tipuri, mai ales dacă semnalul rezultat e amplificat și corectat la locul de ascultare.

Dacă este adevărat ce s-a consemnat, pentru România era o realizare tehnică remarcabilă, un salt calitativ, care nu se putea obține decât pe baza unei acumulări de experiență, chiar dacă era vorba de un domeniu mai puțin "curat", cel al interceptării convorbirilor. Această experiență a fost câștigată prin activitatea desfășurată în această specialitate în perioada dintre cele două războaie mondiale. Telefonul urmărit trebuie să fie sunat de la locul de ascultare și după terminarea convorbirii și închiderea lui, el rămânea "agățat" de chemător și astfel acesta, putea auzi ce se vorbește în jurul microfonului cu cărbune din telefonul modificat. Pentru serviciile specializate, se pot imagina și alte sisteme de a ține permanent "agățat" telefonul supravegheat.

Odată cu progresul tehnic, în special prin apariția tranzistoarelor, s-a ajuns atât la miniaturizare cât și la o fiabilitate ridicată a dispozitivelor de interceptare. Dezavantajele calitative ale "bătrânului" microfon cu cărbune subalimentat l-au făcut să treacă în galerie Muzeului tehnic iar folosirea microamplificatorului cu tranzistoare a permis să se obțină o calitate deosebită a ascultărilor, putându-se intercepta, cu rezultate bune și în deplină siguranță, cel puțin față de persoanele urmărite, atât convorbirile telefonice cât și discuțiile purtate în camera respectivă.

Atâta timp cât amplificatoarele, pentru toate aplicațiile,

s-au realizat cu lămpi electronice iar cele cu două-trei etaje folosite în scopul la care ne-am referit aveau dimensiunile minime cât jumătatea unul pachet de țigări, ne imaginăm ușor că nu puteau fi ascunse într-un telefon. Dacă la acestea, mai adăugăm consumul electric mare, care nu putea fi "suportat" din rețeaua telefonică fără ca aceasta să nu se sesizeze la C.T.A. înțelegem de ce a trebuit să se aștepte apariția tranzistoarelor, apoi a circuitelor integrate, pentru a se realiza microamplificatoare în scopul ascultării secrete a convorbirilor cu ajutorul aparatului și circuitului telefonic. Renunțându-se la folosirea microfonului cu cărbune care a fost singurul mijloc de ascultare, până în anii 1954 - 1955, nu a mai fost nevoie nici să se scurtcircuiteze întrerupătorul, pentru că amplificatorul poate fi plasat în telefon, în "amonte" de contactul furcii telefonului, înspre linie sau chiar pe cablu, înaintea conectării acestuia la aparat. Termenul de "amonte" întrebuițat este folosit ținând seama de sensul de curgere al curentului electric de la C.T.A. spre telefon. Amplificatorul, de dimensiuni ce se încadrează într-un volum de sub 10 cm^3 , prevăzut cu microfon miniaturizat cu un volum în jur de $0,5\text{ cm}^3$, poate fi ascuns în foarte multe piese componente ale telefonului, în condensatorul acestuia, în microreceptor, în rozetă și nu numai în acestea. Are un consum de câțiva zeci de miliwați, curentul de alimentare fiind sub cel necesar microfonului cu cărbune subalimentat. Valoarea semnalului de audiofrecvență la ieșirea din amplificator este suficient de mare pentru o bună transmisie telefonică (între 0,5 și 1 V). Stim că, în momentul când posesorul telefonului interceptat dorește să vorbească și ridică microreceptorul, datorită consumului microfonului cu cărbune, tensiunea scade de circa patru ori. Amplificatorul, care este permanent conectat pe circuit, poate fi proiectat să nu mai funcționeze la această tensiune redusă și astfel să nu deranjeze convorbirea telefonică. Sigur, se pot găsi și alte rezolvări tehnice, care se vor trata în cele ce urmează. Este bine să se rețină însă faptul că, indiferent unde se montează amplificatorul cu microfonul său în telefon, în rozetă, sau undeva pe cablul telefonic, el interceptează convorbirile care se poartă la o distanță de până la circa patru metri (într-un spațiu închis) de locul unde acesta din urmă se află plasat. Deci, ne referim la locul unde se află microfonul și nu amplificatorul, pentru că deși în foarte multe cazuri acestea sunt montate împreună, există situații, când

amplificatorul este plasat într-un loc, pentru a putea fi branșat și eventual schimbat ușor, în mod secret, pe cablul telefonic, iar microfonul, legat prin două fire ecranate de amplificator este montat la câțiva metri, acolo unde se știe că vor avea loc discuțiile ce interesează (cazul când telefonul cu cablul său se află în holul unui apartament și discuțiile se poartă în camera de zi sau în dormitor). Se ridică această problemă pentru că, fie din necunoaștere, fie pentru dezinformare, în multe filme, pentru a fi sigur că nu ești ascultat, se sugerează să se acopere aparatul telefonic, fie și cu o pernă, dar după cum am văzut, microfonul poate fi și în altă parte. Totuși, se ridică unele întrebări. De ce astfel de dispozitive se montează în telefon, când nu este obligatoriu să fie plasate în aparat ? Sau, de ce se folosește ca suport pentru transmiterea la punctul de ascultare, cablul telefonic, pe care se află în funcțiune un telefon ? Răspunsurile la aceste întrebări sunt următoarele: se plasează, de foarte multe ori în telefon, pentru că este comod, fie că se înlocuiește, chiar sub privirile "abonatului" cu altul dinainte "aranjat", fie că se schimbă numai piesa din telefon așa-zis defectă, cu alta care conține însă și amplificatorul. Chiar dacă este necesar, pentru a elimina orice suspiciune, să se pătrundă în mod secret în birourile unei companii rivale, poate și cu "bunăvoința" cumpărată a paznicului, în cadrul unor acțiuni de spionaj sau contraspionaj economic, operația de plasare a dispozitivului de interceptare în telefon durează doar câteva minute.

Să ne imaginăm cât de dificil ar fi să montăm un astfel de amplificator de ascultare într-o încăpere fără telefon, fie în zid, fie în parchet, în tocul ușii sau mobilier și să refacem totul pentru a nu lăsa urme. Operațiunea nu e imposibilă, dar ea durează câteva ore, cu riscurile respective. Si totuși, de ce pe cablul telefonic ? Pentru că, folosindu-l, avem asigurată ieșirea din clădirea din care se face interceptarea. Să ne gândim că altfel, de la amplificator, odată instalat, mai trebuie să "pozăm" (montăm) un cablu special până la punctul de ascultare, prin care să realizăm atât alimentarea cât și transportarea semnalului util captat. Nu este simplu și cred că am dat suficiente date prin care să se înțeleagă comoditatea folosirii telefonului și a circuitelor "ocupate" (cu posturi în funcțiune). Cablul telefonic indiferent până unde-l folosim, în traseul lui spre C.T.A. este un element ideal pentru a ieși dintr-o clădire, bineînțeles în asemenea scopuri. Oare la acest

sistem mai sunt necesare perfecționări ? Răspunsul este afirmativ, în sensul măririi gradului de asigurare a secretului operațiunii, în special față de cei supravegheați, dar și față de compania de telefoane. În unele situații, se are în vedere, chiar cu riscul, sofisticării aparaturii de la locurile intermediare sau finale de ascultare, să se simplifice soluția folosită pentru realizarea aparaturii plasate la locul de interceptare și să se ușureze la maximum montarea ei.

O secretizare superioară

În scopul arătat mai sus, pentru a mări secretizarea acțiunii și a nu crea nici o bănuială abonatului interceptat, s-a căutat să se realizeze tehnic cerința ca, în momentul când telefonul nu funcționează și prin el și circuitul său se realizează numai ascultarea "interioară" a convorbirilor, acesta să fie alimentat direct printr-un circuit telefonic, nu de la centrală ci de la locul de ascultare, cu ajutorul unui transformator special și a două contacte duble ale unui releu, cu o tensiune de aceeași valoare (48 V) cu cea de alimentare din C.T.A.

- În această situație, eventualele măsurători făcute de către Compania de telefoane pentru depistarea instalațiilor de ascultare va indica prezența normală a unui telefon, cu microreceptorul pe furcă, ce nu consumă de la centrală nici un curent. Deci, se poate decide că nu există dispozitive de interceptare. În momentul când abonatul folosește telefonul, consumul din baterie crește brusc de la 3-5 mA, câți sunt necesari amplificatorului, la zeci de miliamperi. Instantaneu, acest curent care trece prin bobina releului, comută circuitul telefonului urmărit pe perechea din cablu, care-l conectează direct, prin repartitor, în sistemele de comutație ale C.T.A. Aceeași operație se întâmplă și când telefonul este sunat. Fără a intra în amănunte tehnice, ne limităm a spune că, pentru a face posibile aceste operații, se înțelege că este necesar ca circuitul telefonului supravegheat să fie dus din repartitorul C.T.A. direct printr-o pereche a cablului special, de care am vorbit la început, până la centrul de ascultare, pentru a se putea realiza comutarea.

Pentru prelungirea telefonului, în sens invers, până la C.T.A. când acesta este în funcțiune, este necesară folosirea unei alte perechi din același cablu multifilar special.

Deci, cum am arătat, din acest cablu ce leagă centrul de ascultare cu C.T.A., se folosesc, de data aceasta, două perechi pentru interceptarea unui singur telefon sau, altfel spus, circuitul telefonic își dublează practic lungimea (Abonat - C.T.A. - Centrul de interceptare - C.T.A.). În aceasta constă și dezavantajul acestei metode. Faptul că circuitul telefonic se extinde (dacă el era și înainte foarte lung și locul de ascultare este depărtat de centrala telefonică) determină ca abonatul să sesizeze diferența calitativă și de volum a audiției, în convorbirile pe care le efectuează, comparativ cu situația când nu era interceptat. Pentru a preîntâmpina astfel de situații, încă de la introducerea dispozitivului de ascultare, cunoscându-se situațiile concrete de amplasare, în condițiile când distanțele sunt foarte mari, sistemul de alimentare, transformatorul și releele cu contacte duble se plasează într-o clădire în apropierea C.T.A., spre centrul de ascultare trimițându-se numai semnalul audio și unele elemente pentru semnalizare și prinderea numerelor de telefon. Deși metoda expusă satisface pe deplin calitatea audiției și gradul de secretizare, totuși necesită plasarea microamplificatorului în perimetrul interceptat care, dacă este depistat, (în special de către tehnicienii ce lucrează în ambasade, sau de către echipe specializate) poate constitui probă pentru a demonstra interceptarea.

Ascultarea fără piese compromițătoare

De aceea, în continuare mă voi referi pe scurt la o altă metodă care, deși până în prezent n-a adus rezultate calitative, ca ale celei descrise mai sus, și-a propus în schimb să rezolve reducerea la minim a volumului și "importanței" piesei care se introduce în telefon. Metoda poartă denumirea în limba engleză "radio frequency flooding" - așa cum o numește autorul lucrării la care m-am referit la începutul capitolului (inundare cu radio-frecvență) și se pare că a fost apreciată mult de serviciile de contraspionaj engleze și folosită în anii '60, împotriva unor telefoane din ambasadele care funcționau la Londra. Un generator de radiofrecvență, dispus în apropierea telefonului interceptat (20 ÷ 30 m), injectează energie în casca aparatului telefonic; are loc, așa cum numesc specialiștii, o modulație prin absorbție; se obține o armonică, ce, reflectată poartă "informația" rezultată din

acțiunea undelor sonore asupra membranei căștii, care este trimisă spre centrul de interceptare. Frecvența se stabilește tot ca un compromis între dorința ca aceasta să fie cât mai mare, pentru a putea trece mai ușor peste contactul nemodificat al întrerupătorului telefonic și între datele constructive ale acestuia (se dorește obținerea unui efect de rezonanță); trebuie ținut seama că pierderile de energie sunt foarte mari pe cablul telefonic la frecvențe ridicate. Se pare, deși în literatura de specialitate nu se dau date precise, că aceasta este în jur de 1-2 MHz. Pentru a ușura trecerea spre casca telefonului, contactul este totuși șuntat cu un condensator de valoare mică, ce se poate contrui chiar din piesele din care este făcut întrerupătorul, prin unele modificări simple ale acestuia ce pot fi realizate chiar în fabricile constructoare, odată cu producția telefonului. Care ar fi motivația acestor modificări ? Așa cum montarea din fabrică a unei diode, paralel pe casca telefonului, la toate aparatele, este motivată ca protecție împotriva unor zgomote puternice și condensatorul la care ne-am referit are o justificare foarte plauzibilă, ca element antiparazit și antiflamă. Astfel, când un abonat își cumpără telefonul, își aduce în casă și dispozitivul de interceptat convorbiri, iar cei ce se ocupă cu astfel de activități nu se mai obosesc să pătrundă în apartamente.

Deoarece am arătat că această metodă era preferată în vestul Europei, pentru a fi imparțial, trebuie spus că, în extremitatea estică a continentului nostru se folosea aceeași metodă, dar cu o frecvență de lucru de circa 30 de ori mai mică ce se injecta în microfonul cu cărbune, în loc de cască. Trebuie arătat, de asemenea, că este lipsită de orice justificare tehnică, bănuială pe care o manifestă foarte mulți abonați că sunt interceptați când aud zgomote pe linie, păcănituri, întreruperi, alte convorbiri (diafonie). Toate acestea se datorează defecțiunilor din centralele telefonice și în special a cablurilor telefonice și anume uzurii izolației și scăderii rezistenței între perechi.

A produs multă stupeoare când un ziarist, cu pregătire politică și culturală, a afirmat în mod public la TV că-i sunt interceptate convorbirile telefonice susținând aceasta cu argumente, de genul sesizării de pârâituri, zgomote și, culmea, chiar de voci ale celor care fac supravegherea !

CAPITOLUL VI

INTERCEPTAREA CONVORBIRILOR CU AJUTORUL MICROFOANELOR ȘI AMPLIFICATOARELOR (MICROFON CU FIR)

În continuare, ne vom ocupa de sistemele de ascultare a convorbirilor, care, spre deosebire de cele care au fost descrise până acum, folosesc, atât pentru alimentare cât și pentru transmiterea semnalului la locul de ascultare perechi de cabluri telefonice pe care nu sunt telefoane în funcțiune (așa-numitele perechi libere).

Se înțelege că nu este obligatoriu să se folosească numai aceste cabluri, ci se pot întrebuința și alte fire, fie existente, fie care se instalează odată cu montarea aparaturii de interceptare. Sunt așa-numitele sisteme "microfon cu fir", unele dintre cele mai vechi, dar care și astăzi se întrebuințează foarte mult, pentru că sunt fiabile și nu prezintă nici o limitare în timp. Instalațiile la care ne referim se compun în principal din microfoane și preamplificatoare tealealimentate.

Microfonul - element de bază al interceptării

Prezentăm acum câteva date despre microfoanele folosite, lăsându-l la o parte pe cel cu granule de cărbune, la care ne-am referit cu ocazia prezentării interceptărilor telefonice. În afară de acestea, primul microfon folosit în astfel de instalații este cel dinamic sau magnetic, cu caracteristici deosebit de bune. El se compune dintr-un magnet permanent, o bobină, care, presată de diafragma mobilă, taie liniile câmpului magnetic, rezultând în ea tensiuni de aceeași frecvență și proporționale ca amplitudine cu cele ale undelor sonore, care "atacă" membrana. Semnalul electric rezultat este preluat de amplificator și transmis până la punctul de ascultare. De foarte multe ori, atât microfonul cât și amplificatorul

sunt construite într-o carcasă comună care are un volum de circa 15 cm^3 , prevăzându-se un loc de adaptare a unui tub din plastic, cu ajutorul căruia să fie captate undele sonore ale conversației interceptate.

Deci, microfonul poate fi plasat într-o cameră alăturată și, cu ajutorul tubului care străbate zidul despărțitor, să capteze conversația dintr-o cameră vecină. Astfel de microfoane dinamice au fost descoperite în Ambasada S.U.A. de la Moscova. Un alt tip de microfon folosit este așa-numitul microfon-cristal, format din două plăcuțe subțiri tăiate dintr-un cristal (de aici și denumirea), "crescut" artificial după o anumită tehnologie, dintr-o soluție suprasaturată de sare de Segnette. Aceste plăcuțe care apoi sunt argintate, au proprietatea ca la presiuni exercitate mecanic - în cazul de față de către o membrană din folie de aluminiu - să livreze tensiunea electrică, proporțională cu frecvența și amplitudinea undelor sonore. Totul este capsulat într-o cutie de protecție din material plastic, lăsându-se în partea frontală o fantă dreptunghiulară de $25 \times 2 \text{ mm}$ în fața membranei, pentru a putea permite intrarea undelor sonore. Este mult mai sensibil ca cel dinamic, are o curbă de răspuns bună, livrează o tensiune mai mare, dar în schimb este mai puțin rezistent la șocuri și umiditate. Conține foarte puțin metal, deci este mai greu detectabil cu aparatura ce semnalizează prezența acestuia.

Deoarece s-a abordat în ansamblu problema microfoanelor, va fi prezentat în continuare și microfonul condensator, cel care nu se întrebuințează de regulă în instalații de interceptare cu fir, ci mai ales în microemițătoare. Este format dintr-o folie circulară, încastrată la margine și un miez central metalic care formează cu membrana (folia) un condensator a cărui capacitate este variată de energia acustică ce acționează asupra membranei. Este microfonul care are cea mai bună curbă de răspuns, indicat atât pentru redarea frecvențelor joase cât, mai ales a celor înalte. În primele microemițătoare construite, acesta este montat chiar în circuitul oscilant. Datorită calităților sale deosebite este considerat microfonul "rege" pentru sonorizarea sălilor de concert.

Astăzi, poate cel mai întrebuințat pentru captarea sunetelor în instalațiile de interceptare este microfonul cu electret care are dimensiunile cele mai mici (de mare importanță în scopurile la care m-am referit), o mare sensibilitate și o bună

curbă de răspuns în frecvență. Din punct de vedere constructiv, seamănă cu cel de tip condensator dar spre deosebire de acesta amplificatorul la care este conectat îl alimentează permanent cu o tensiune electrică care este variată în funcție de semnalul audio, rezultând astfel semnalul care va fi amplificat. Este neinfluențat de perturbații magnetice întâmplătoare sau provocate ca măsuri de contracarare a interceptărilor și este foarte greu să fie depistat de echipe specializate în detectarea instalațiilor de ascultare.

Fabricarea microfoanelor este o afacere foarte rentabilă și multe firme occidentale, spre exemplu "Shure" și "Knowless" dar și altele, au câștigat numai din aceste produse milioane de dolari. Si când te gândești, că din produsele fabricate, peste 40% se cumpără în scopurile la care m-am referit și nu pentru săli de concert, instalații de amplificare și radiodifuzare sau pentru aparatura necesară hipoacuzilor !

Având în vedere situațiile pe care și le propune să le rezolve, mai există două categorii de microfoane. Prima se referă la cele care preiau vibrațiile unor ziduri subțiri (uși, geamuri) datorate undelor sonore rezultate din convorbirile ce urmează să fie interceptate și pe care le transformă în semnale electrice.

Din punct de vedere al principiului de funcționare al microfonului propriu-zis nu sunt deosebiri față de cele pe care le-am descris mai înainte, în special față de microfonul-cristal. Pentru a crea posibilitatea ca vibrațiile mecanice să preseze asupra plăcuțelor de cristal, s-au imaginat diferite soluții constructive, fie sub forma unor cavități, fie a unor țepușe a căror parte ascuțită se plasează pe suprafața care vibrează. Aceste microfoane, numite generic de "contact" se întrebuințează la instalațiile de interceptare pentru durate scurte, dintr-o cameră în alta sau acolo unde nu a existat timpul material pentru a realiza o instalație "clasică" de ascultare.

A doua categorie de microfoane se referă la cea care își propune să realizeze captarea sunetelor în aer liber de la distanță. Acestea se fabrică în două modele. Primul seamănă foarte mult, ca formă, cu antenele parabolice din instalațiile de captare a transmisiilor prin satelit și cel de-al doilea este format din mai multe tuburi paralele, de lungimi diferite; de aici și denumirile de microfon-parabolic, respectiv microfon-pușcă. Trebuie spus că acestea sunt mai mult rezolvări teoretice cu aplicații pentru condițiile ideale, mai puțin pentru situațiile concrete, reale. Pentru

a le folosi în scopuri practice, cu rezultate mulțumitoare, ar fi necesară o antenă parabolică cu diametru de câțiva metri. Este greu de imaginat că o asemenea instalație, cu toate măsurile de camuflare nu poate fi observată de cei ce urmează să fie ascultați. Ideea folosirii acestora a fost preluată de la ornitologi care le foloseau în studiul limbajului păsărilor, dar în astfel de situații nu există surse perturbatoare și "trilurile" păsărilor au componente predominante în frecvențe mai înalte decât cele ale vocii umane, ceea ce face necesară o antenă cu diametrul mai mic.

Amplificatoare folosite în Interceptări secrete

Dar să lăsăm deoparte ornitologii și să revenim la problema pe care ne-am propus s-o tratăm. Amplificatoarele folosite în astfel de scopuri nu prezintă probleme deosebite. Ele pot fi cumpărate sau construite de către tehnicieni electroniști din componentele ce se găsesc pe piață. Este interesant de arătat că atunci când dorim să interceptăm convorbiri care se pot purta în oricare din încăperile unui apartament - pe rând - și nu vrem să folosim pentru fiecare cameră un amplificator sau, în special, să nu ieșim cu 4-5 perechi de fire din apartament, atunci, între microfoane și amplificator sau între amplificatoare și o pereche comună de ieșire, se intercalează un comutator de microfoane, respectiv de amplificatoare. Se realizează astfel performanța ca pe o singură pereche de fire să se alimenteze și să se comute patru-cinci instalații putându-se asculta, la dorință, fiecare din acestea (după camera în care se poartă discuția). La locul de ascultare există o masă-pupitru cu 30-40 instalații concentrate ca cea care s-a descris când s-au făcut referiri la instalațiile de interceptare a convorbirilor telefonice, la care se poate sesiza optic sau acustic, faptul că într-o cameră interceptată au loc convorbiri. "Masa" mai dispune de dispozitive acustomat pentru comanda înregistrării convorbirilor. Prin apăsarea unui simplu buton, aflat pe masa-pupitru se pot comuta ascultările convorbirilor din fiecare cameră a unui apartament. S-ar părea că este o culme a eficienței acestei activități. Afirmatia nu este departe de adevăr și se pare că după interceptarea convorbirilor telefonice, aceste sisteme botezate "microfon și cu fir" sunt cel

mai mult întrebuințate de instituțiile guvernamentale specializate, în obținerea informațiilor de la ambasade, alte instituții și întreprinderi străine precum și de la funcționarii acestora.

Primele informații despre folosirea acestora s-au obținut imediat după cel de-al doilea război mondial, când s-a făcut public faptul că ele erau în "dotarea" fiecărui apartament de la saloanele cu fete (gen kity). Interceptările erau efectuate de Gestapo în principalele orașe din Germania, cu deosebire în Berlin, pentru a-și asculta proprii ofițeri aflați în misiune în capitala țării, ori străinii care mai activau în Germania în perioada 1942 - 1945. Dar să prezentăm și exemple mai recente. Un recent șef al Serviciului de Informații rus, Vladimir Bakatin, numit în funcție după puciul militar din U.R.S.S., întrebat fiind despre interceptările telefoanelor folosite de instituția pe care o conduce, s-a referit în schimb la faptul că, atunci când funcționa ca atașat de presă la Londra, a găsit în apartamentul său din Capitala Marii Britanii, instalații de ascultare de tip "microfon cu fir". Aceleași instalații au fost descoperite, tot după spusele sale, de echipe sovietice specializate în locuințele unor delegații comerciale ale U.R.S.S., care purtau tratative în Anglia (din păcate sursa nu precizează anul). Instalațiile descrise, pe lângă avantajele prezentate, au o limită și anume aceea că, dacă perechea prin care se părăsește apartamentul și care "transportă convorbirile", este depistată, cu o simplă cască, sau alt dispozitiv de ascultare, ea se poate intercepta și asculta. Există și pentru acest inconvenient soluții la care ne vom referi.

Rețeaua electrică - suport ideal pentru interceptare

Pentru a înlătura dezavantajul la care s-au făcut referiri, așa cum rezultă din puținele lucrări de specialitate publicate, din cataloagele firmelor producătoare, s-a recurs la metoda curenților purtători, folosită mai ales în telefonie la mare distanță. Semnalul, care este livrat de amplificatoarele de la instalațiile de interceptare "modulează", (vom explica ulterior acest termen tehnic) o tensiune a cărei frecvență este foarte mare față de cea a semnalului vocal (de douăzeci-treizeci de ori), dar în același timp foarte mică, dacă o comparăm cu cea a frecvențelor folosite în

transmisiunile radio. Aceasta "poartă" informația pe cablu, până la punctul de ascultare și are avantajul că nu radiază decât foarte puțină energie în eter, pentru a putea fi captată cu receptoare, chiar dacă acestea au aceleași benzi de frecvență. Ea nu poate fi nici ascultată cu dispozitive simple (cască, amplificatori), în cazul în care se controlează perechile din cablu prin care se face transmiterea, ci numai cu un dispozitiv de recepție special construit, cu bandă de frecvență (50-300 KHz) și care realizează și demodularea în frecvență. Pe lângă acest avantaj, tipul de instalație de ascultare pe care îl prezentăm, oferă celui care îl folosește posibilitatea să nu mai aibă nevoie de un cablu special de ieșire din apartamentul unde s-au montat dispozitivele de interceptare ci este suficient să folosească cablul de alimentare electrică. Cu ajutorul lui se reușește să se rezolve cea mai grea problemă și anume scoaterea semnalului util din încăperile controlate.

Apoi, "convorbirea" este reluată tot din cablul electric de la oricare alt apartament al imobilului ori dintr-o clădire apropiată. Ascultarea se desfășoară în locul de preluare, ori semnalul este prelucrat și trimis până la centrul de interceptare prin oricare alt mod. Dacă drept suport de transmisie al informației este folosit cablul electric, se impun două modalități de interes practic. Mai întâi, dispozitivele de interceptare pot fi camuflate în obiecte care, de obicei, stau introduse permanent în prizele electrice (veioze, cabluri prelungitoare, aparate de radio, TV etc. (fig. 5). În al doilea rând, datorită faptului că este instalația ideală pentru a intercepta convorbirile dintr-o cameră de hotel, se poate înlocui o veioză din dotarea hotelului, cu o alta de același tip și formă, dar care are în ea montată instalația de interceptare. Ascultarea, în acest caz, se poate realiza din foarte multe alte camere (unde se regăsește aceeași fază a cablului electric). Se deduce ușor că acest tip de instalație este foarte indicat pentru a realiza o legătură impersonală între doi agenți care își schimbă informațiile fără a se întâlni.

Si cu aceasta s-a pus punct prezentării principalelor tipuri de instalații de captare a convorbirilor, care apoi sunt trimise la locul de ascultare, pe cabluri, fie că acestea sunt telefonice sau electrice, așa-numitele ascultări cu fir.

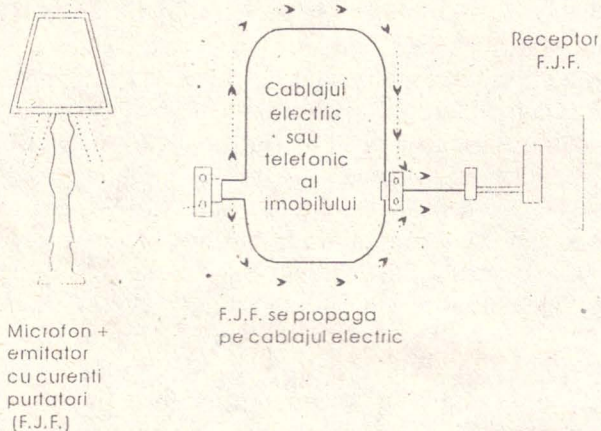
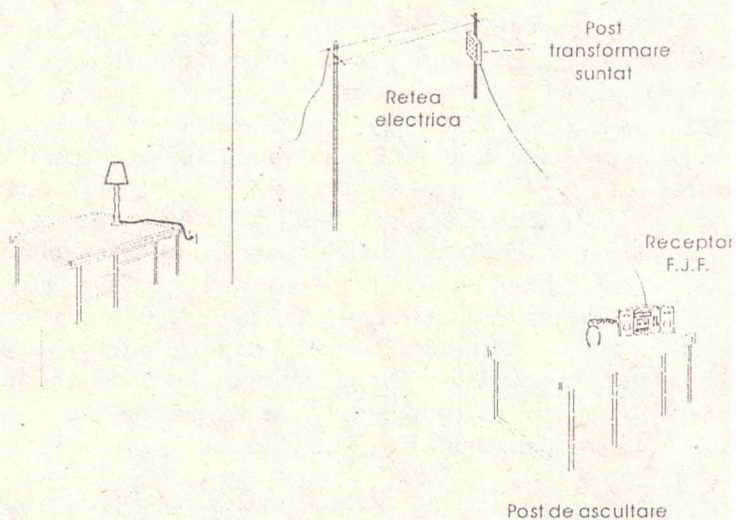


Fig. 5. Interceptare cu curenti purtatori

CAPITOLUL VII

MICROEMIȚĂTOARE - MICROFOANE FĂRĂ FIR

Concomitent cu folosirea instalațiilor prezentate, poate în cazuri și mai numeroase, mai ales când este necesar să fie interceptată o convorbire de scurtă durată - câteva ore - într-un local public, sau atunci când nu este timpul necesar pentru a realiza o instalație cu fire se folosesc microemițătoare care transmit informațiile până la punctul de ascultare prin eter. Recent, presa din țara noastră a relevat, fără a lămuri pe deplin, că discuțiile purtate într-un birou al unui minister din București, ar fi fost interceptate dintr-un autoturism. Dacă este adevărat, la astfel de instalații de interceptare se făceau referiri. Acum vreo douăzeci de ani a făcut multă vâlvă cazul unui fost membru al Partidului Comunist Bulgar care, recrutat de serviciile de spionaj ale unei țări occidentale, se ducea la ședințele plenare având asupra lui un microemițător, transmițând astfel cele ce se discutau și care erau interceptate dintr-un autoturism dotat cu receptor și magnetofon de înregistrare. Nu ne ajunge hârtia să descriem câte alte cazuri de interceptări cu ajutorul microemițătoarelor au existat și care au fost mediatizate. S-au interceptat convorbiri purtate în restaurante, ședințe importante ale unor consilii de administrație ale unor firme, discuții dintre diverși "trimiși" și personalul unor ambasade. S-au obținut probe în cadrul unor întâlniri amoroase extraconjugale pe care dorea să le posede unul dintre soți etc. Iată o relatare în revista "Science et vie" (iunie 1992) la care am mai făcut referiri privind microemițătoarele sub titlul: "*Spionii în birou*". Redăm traducerea integrală a acesteia: "Este ușor de camuflat într-un obiect obișnuit un microemițător care transmite sunetele captate sub formă de impulsuri electrice. Microemițătorul este alcătuit dintr-un microfon legat de un emițător miniaturizat, aflat într-o cutie, în care s-a practicat un mic orificiu la nivelul microfonului, cu o antenă exterioară sau inclusă, alimentarea fiind asigurată de baterie. "Bătaia" acestor aparate comercializate de către societatea Confrexport variază în funcție de puterea de emisie de la 15 la 20 m pentru știlou, 25 m pentru scrumieră..."

Să lăsăm părerile ziariștilor și să încercăm o prezentare mai metodică. Înainte de a descrie aceste microemițătoare este absolut necesar, fără să abuzăm de termeni tehnici, să lămurim ce este modulația și banda de frecvență în care funcționează aceasta. Să ne imaginăm o sursă de lumină care reprezintă suportul material al transducerii informației și pentru a realiza, stingem și aprindem lumina după un anumit cod (spre exemplu Morse). Putem spune că lumina a fost modulată de tipul stins, aprins (cu timpi diferiți) și am reușit să transmitem informații. Dacă, în loc de lumină, ne imaginăm o radiație electromagnetică produsă de un oscilator și procesul de modulație cuprinde nu numai valorile extreme, maxim (lumina aprinsă) și minim (lumina stinsă) de amplitudine ci și valori de intensitate care respectă amplitudinea și frecvența informației (a vocii umane, a unor sunete muzicale și chiar a unor zgomote pe care vrem să le transmitem), spunem că am realizat modulație de amplitudine care acționează numai asupra intensității (amplitudinii), semnalului purtător. Această modulație se folosește în cazul transmisiilor radio în unde medii (530 - 1600 KHz). Dacă însă, variază nu amplitudinea semnalului purtător, ci frecvența centrală a acestuia între anumite limite, spunem că am realizat modulația de frecvență și acest procedeu este folosit în radiodifuziune pentru posturile FM din banda de frecvență cuprinsă între 60 - 108 MHz, precum și în microemițătoarele de interceptare ce ne interesează pe noi, care funcționează în special în jurul frecvențelor de 150MHz, 400 MHz și chiar 900 MHz.

După cum s-a mai arătat, datorită faptului că aceste microemițătoare transmit informațiile la locul de ascultare prin radiații electromagnetice propagate prin eter, ele mai sunt denumite "microfoane fără fir" (wireless microphones). Principalele părți componente sunt: oscilatorul de radio-frecvență, care generează purtătoarea, modulatorul și amplificatorul de audiofrecvență. Le-am prezentat pentru că de multe ori, pentru a nu fi acuzați că fabrică și comercializează astfel de dispozitive "imorale" producătorii le livrează sub formă de părți componente,

utilizatorul neavând altceva de făcut decât să le assembleze după o schemă ce poate fi obținută la cerere.

Puterea microemițătoarelor de interceptare este diferită, (de ordinul miliwaților) și asigură o "bătăie" în jur de o sută de metri. Aceasta se stabilește în urma unui compromis între dorința, ca pe de o parte, distanța până la care pot fi recepționate să fie cât mai mare, și pe de altă parte, necesitatea de a nu fi "prinse" accidental sau voit de alte receptoare și de asemenea, între dezideratul ca dimensiunile acestora să fie cât mai mici și puterea să fie cât mai mare (ceea ce ar implica și un volum mare).

Dimensiunea și puterea acestui tip de emițător sunt determinate în cele din urmă de volumul bateriilor care-l alimentează. Progresele făcute în domeniul componentelor electronice care au dus la construirea unor emițătoare foarte mici n-au fost susținute cu aceleași rezultate spectaculoase în domeniul bateriilor de alimentare. Celebrele firme Mallory, Vatra, Ever-ready, Duracell, cu toate succesele obținute, n-au reușit să fabrice pile (baterii) electrice pe măsura dorințelor și necesităților. Dacă s-ar fi realizat baterii performante ar fi credibilă publicitatea care se face în jurul faptului că aceste emițătoare pot fi plasate și în pahare cu băuturi. Adevărul este că au rămas foarte puține obiecte care pot exista în locurile în care se poartă o discuție și în care să nu se fi montat astfel de emițătoare. De obicei, acestea sunt "găzduite" în scrumiere, farfurii, cuțite, în toate ustensilele de birou, în stilouri, dar cel mai mult este întrebuințată mascarea pe care au încercat-o organele de informații cehe, atunci când au dorit să plaseze instalații de interceptare în clădirea Departamentului de stat al S.U.A. și anume, un paralelipiped de lemn scobit, ca un penar în care se pot plasa și mai multe baterii, pentru o mai mare durată de funcționare, de la câteva ore, până la câteva zile. Un asemenea obiect poate fi prins sub orice mobilier care se poate afla într-o încăpere (birou, dulap, fotoliu, pat etc.). Pentru a elimina neajunsurile cauzate de viața limitată a bateriilor s-au construit emițătoare alimentate la rețeaua electrică având o durată de funcționare practic nelimitată. Acestea sunt camuflate în obiecte care stau tot timpul sub tensiune și sunt racordate, în mod ascuns, la rețeaua electrică, în spatele unor prize electrice sau în alte locuri pe traseul invizibil al rețelei electrice. Primele emițătoare s-au construit în banda de radiodifuziune de 88 - 108 MHz ca să nu mai necesite receptoare

speciale și să fie suficientă folosirea celor obișnuite, din comerț. Dar, pentru că astfel de receptoare au devenit foarte răspândite și există pericolul să se intercepteze convorbirile și de către persoane neavizate, s-a renunțat și s-a trecut în banda de 150MHz, apoi la cea de 400 - 475 MHz și, în final, la cea de 900 - 1000 MHz. Pe măsură ce au fost folosite frecvențe mai mari, a crescut calitatea audiției, s-au eliminat sursele perturbatoare, s-a micșorat antena etc. Pentru a elimina inconvenientul acestor dispozitive, în special a celor de la început și anume instabilitatea frecvenței (fuga de pe post) s-a acționat pe două direcții: fie prin montarea unui "cristal", care să controleze frecvența pilot a emițătorului, fie prin introducerea controlului automat de frecvență la receptoare (C.A.F.).

Se cunoaște că principalul inconvenient al acestui sistem de interceptare îl constituie faptul că poate fi recepționat și depistat, chiar și accidental, fără să mai vorbim de detectarea organizată de către echipe specializate, dotate cu echipament corespunzător. Există receptoare de control pe toate benzile, ce pot efectua baleierea automată (parcurerea frecvențelor), care se opresc și comandă înregistrarea când găsesc un emițător în funcțiune. Ele pot fi programate să "sară" peste anumite posturi de radiodifuziune cunoscute și memorate în prealabil.

Perfecționarea emițătoarelor pentru asigurarea securității interceptărilor

Pentru a se apăra împotriva acestor "inamici", constructorii de emițătoare au luat unele măsuri de protecție. Astfel, s-au proiectat și realizat, în primul rând, dispozitive telecomandate. Acestea dispun, pe lângă emițătorul propriu-zis, de un receptor de dimensiuni foarte mici care, în funcție de comanda pe care o primește, pornește sau scoate din funcțiune emițătorul de interceptare.

Comandarea receptorului se face de la câteva sute de metri de către un emițător de 1 - 2 W.

Se obține, pe de-o parte o viață mai lungă de funcționare, prin economisirea bateriilor și în al doilea rând, emițătorul funcționând numai atât cât interesează convorbirile care se poartă, se determină implicit și reducerea perioadei de emisie, deci și a posibilității de interceptare. Atunci când astfel de emițătoare

sunt instalate în ambasade, unde acționează periodic echipe de specialiști pentru căutarea și depistarea lor și când se cunoaște, momentul începerii activității, emițătoarele sunt scoase în prealabil, obligatoriu din funcțiune, pentru a nu fi descoperite. Tot pentru a "îngreuna" ascultările nedorite, se folosesc procedee mai complicate de modulare a semnalului la emițător. Este vorba de așa-numita tehnică a subpurtătoarei.

Astfel, frecvența audio se combină cu o oscilație, denumită subpurtătoare, în jur de 75 KHz iar rezultatul obținut va modula purtătoarea de radiofrecvență care va fi emisă în eter cu ajutorul antenei. În cazul când acest semnal va fi recepționat, accidental sau voit, cu un aparat obișnuit, cu simplă demodulație, nu se va înțelege semnalul util. Uneori se iau măsuri și mai complexe, pentru ca tehnicianul ce caută să descopere emisiunile respective, să audă o frecvență de 800 - 1000 Hz, exact semnalul emis în mod obișnuit de un post de radiodifuziune oficial care se pregătește să-și înceapă programul.

Astfel, se intenționează și se reușește de foarte multe ori, inducerea în eroare a celui ce ascultă, crezându-se că este vorba de un post de emisie autorizat. O altă metodă de protecție pe care o folosesc cei ce fac interceptări și care este descisă în manualele de specialitate, este denumită "Smuggling" (a ține în brațe). Frecvența emițătorului se alege foarte aproape de cea a unui post de radiodifuziune local. Dacă cel ce execută controlul posedă un receptor de tip clasic, cu control automat de frecvență (C.A.F.) când explorează banda "sare" peste postul clandestin, care este de mică putere și îl recepționează numai pe cel de radiodifuziune. De aici și denumirea dată metodei, care înseamnă că postul puternic "ține în brațe" (ascundé) pe cel de interceptare.

*

* *

S-a prezentat faptul că acest sistem de interceptare poate fi folosit cu ajutorul unor "trimiși" pentru a intercepta discuțiile care se poartă acolo unde aceștia participă. Ei sunt purtătorii microemițătoarelor care captează convorbirile și le trimit apoi prin eter la punctul de ascultare.

În același timp s-a arătat despre vulnerabilitatea

microemițătoarelor și anume despre recepționarea lor accidentală sau voită de către terțe persoane. În aceste condiții se naște întrebarea: de ce se folosesc în situația prezentată microfoane fără fir și nu se apelează la mini-magnetofone așa cum procedează ziariștii când se duc la conferințe de presă. Răspunsul este complex și cuprinde mai multe aspecte. În primul rând trebuie reținut faptul că este vorba de o înregistrare secretă, când cei care discută nu trebuie să cunoască că sunt ascultați și de alte persoane decât de cele prezente și deci, mini-magnetofonul nu poate fi pus la vedere ca în cazul conferințelor de presă. Acesta este mult mai voluminos decât un microemițător și de aici existența unor greutăți în mascarea lui. El are o durată de înregistrare limitată la 15 ÷ 90 minute, după care purtătorul trebuie să aibă posibilitatea, ca în mod secret, să întoarcă sau să schimbe caseta cu bandă magnetică. În cazul folosirii microemițătorului, cel sau cei care ascultă la punctul de interceptare au posibilitatea să "participe" în direct (live - în timp real) la ceea ce se întâmplă în locul unde se poartă discuțiile și să poată interveni dacă este necesar și să nu se aștepte până la terminarea acțiunii când se întoarce "trimisul" cu banda înregistrată. Și mai este o problemă care de multe ori constituie scopul principal al folosirii microfonului fără fir. Într-un obiect portabil (ex: o servietă) se montează în mod ascuns, fără să cunoască "trimisul", microemițătorul precum și un mini-magnetofon care urmează să fie acționat (pornit-oprit) de către purtător. Din compararea celor două înregistrări realizate, prin cele două sisteme, una făcută la latitudinea "trimisului" (agentului) și alta fără știrea lui se poate deduce ușor loialitatea sau duplicitatea informatorului față de serviciile secrete care-l folosesc. Este poate una dintre cele mai eficace metode de verificare a informatorilor. Ofițerul de informații sau contra-informații folosind una sau alta din sistemele de interceptare, chiar pe amândouă așa cum s-a văzut, alegând locul de plasare al fiecăruia în obiecte portabile sau în îmbrăcămintea agentului, poate rezolva multiple situații operative.

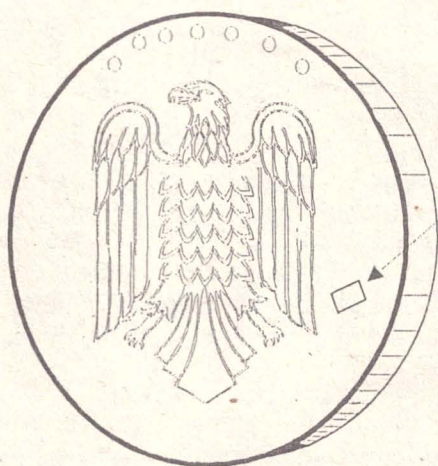
CAPITOLUL VIII

DISPOZITIVE PASIVE

Cititorii își amintesc că la începutul lucrării s-a prezentat succint scandalul datorat descoperirii tehnicii din stema americană aflată în biroul Ambasadorului S.U.A. de la Moscova și campania în presa occidentală în legătură cu mai recenta (la diferență de 30 de ani) "bombardare" cu energie electromagnetică de foarte înaltă frecvență a aceleiași clădiri - Ambasada S.U.A. din capitala fostei U.R.S.S.

S-a anticipat astfel descrierea unui sistem foarte perfecționat de interceptare care se află numai la îndemâna instituțiilor guvernamentale. Este vorba de așa-numiții reflectori pasivi, niște cavități rezonante (ca să reflecte cât mai mult), care posedă o antenă și o membrană ce vibrează la undele sonore ale convorbirilor interceptate. Aceste dispozitive n-au componente electronice și nici un fel de alimentare, deci au durată de funcționare nelimitată.

Poate este greu de crezut că această cavitate care în fond este un simplu cilindru metalic argintat și pentru cazul prezentat avea un diametru de 18 mm și un fir ce reprezenta antena de 240mm, fără nici o baterie, tranzistor, condensator etc., să poată fi folosită în scop de interceptare a convorbirilor. Totuși, dacă cavitatea este "bombardată" cu energie care, în cazul amintit, avea frecvența de 330 MHz, o va capta și o mică parte va fi reflectată prin antena la care ne-am referit. Astfel, undele radio ce provin de la dispozitiv, odată cu reflectarea și-au "adăugat" și "informațiile" primite de la vibrațiile membranei, care respectă toate caracteristicile tehnice ale sunetelor interceptate. Se înțelege ușor că, în cazul în care "bombardamentul electronic" a fost oprit, nu se mai produce nici fenomenul de reflecție și nici de modulare. Pentru a transmite energia de foarte înaltă frecvență sunt necesari emițători de înaltă putere, de ordinul a zeci, sute de KW, care să lucreze în impulsuri. În campania de presă respectivă se arată că se identificaseră și antenele acestor emițători care "bombardau"



Dispozitiv de interceptare

Cavitate pasiva montata in stema de la Ambasada S.U.A. de la Moscova

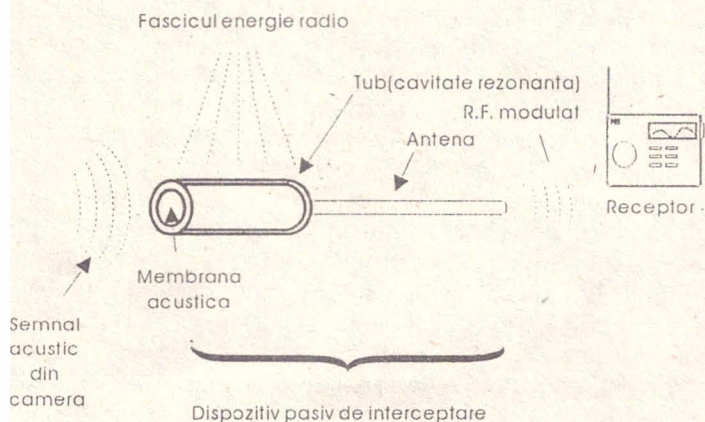


Fig.6 Interceptare cu cavitati pasive

cu unde Ambasada americană și care se aflau pe unele clădiri (din apropiere), mai înalte și mascate de construcții din material plastic, așa-numitele radoame. Descoperind acestea, măsurând și prezența energiei de foarte înaltă frecvență s-a tras și concluzia logică că bombardarea servește, fie la activarea unor dispozitive pasive (fără alimentare), fie mai probabil la punerea în funcțiune a unor reflectori pasivi ca cei pe care i-am descris mai sus.

S-au epuizat astfel, pe scurt, bineînțeles, sistemele de interceptare care folosesc pentru transmiterea semnalelor interceptate energia electromagnetică de frecvențe diferite.

În continuare ne vom ocupa de cele care utilizează sistemele optice și energia luminoasă. În acest domeniu, cel mai mult s-a vorbit de folosirea laserilor, la care ne vom referi în capitolul următor.

Și familiilor regale le sunt interceptate convorbirile

Până aici, am parcurs majoritatea tehnicilor de interceptare a discuțiilor. Recentul scandal din Marea Britanie provocat de publicarea conținutului convorbirilor telefonice dintre prințul și prințesa de Wales ne oferă prilejul de a prezenta luările de poziție și afirmațiile presei engleze pe această temă. Este interesant acest lucru pentru că, în primul rând se trec în revistă toate mijloacele tehnice ce puteau fi folosite pentru interceptare și asta, ca un rezumat al conținutului capitolelor care au fost parcurse. Apoi, aprecierile despre rolul serviciilor de informații engleze în această afacere, controlul acestora de către Parlament, sarcinile și profesionalitatea lor arată că, nu numai la noi în țară astfel de probleme sunt de actualitate, ci și în țări în care democrația și statul de drept nu pot fi puse în discuție de mult timp. Cerem scuze pentru redarea telegrafică, datorită lipsei de spațiu. Ziariștii care susțin că interceptarea a fost executată de către serviciile de informații britanice afirmă următoarele, în cunoscutul cotidian englez "The Independent", din 13 mai 1993, în articolul intitulat "Dacă nu a fost M.I. 5 atunci cine a fost" pe care îl redăm în rezumat:

"Kenneth Clarke a comis o eroare dezmințind neîntârziat o știre apărută în publicațiile "Sun" și "Daily mirror" cu privire la

faptul că serviciile secrete au înregistrat convorbirea dintre prințul și prințesa de Wales. Fără să își rezerve timpul necesar pentru a verifica, ministerul de interne (K.C.) a etichetat această știre ca fiind un "nonsense".

"Mai mult decât atât, exprimându-se în termeni care au constituit o ofensă la adresa capacității de înțelegere a opiniei publice, a comparat această știre cu o 'istorie' veche apărută în presa de scandal, referitoare la un bombardier B-52 descoperit pe lună".

"Afirmările sale au fost susținute și de sursele de la 'Downing street', care au exclus orice posibilitate de implicare a M.I. 5".

"Nu este prima dată când dl. Clarke adoptă o astfel de atitudine. În luna ianuarie, a catalogat ca fiind 'o afirmație prostească', faptul că M.I. 5 sau GCHQ (Centrul Guvernamental de Interceptare a Comunicațiilor din Cheltenham) ar fi fost implicate în înregistrarea așa-numitei convorbiri Camilia Gate..."

"În același spirit, în urmă cu două săptămâni, Guvernul a declarat că datorită a două rapoarte întocmite de înalți magistrați, serviciile secrete sunt absolvite de orice implicare în astfel de probleme".

"La o verificare mai atentă, rapoartele cu privire la înregistrările convorbirilor telefonice, precum și cele referitoare la serviciile secrete exprimau cu totul altceva".

În același cotidian englez se arată în continuare:

"Este foarte clar ceea ce Guvernul are de făcut. Dacă nu știe cine este responsabil pentru aceste înregistrări, ar trebui să instituie o comisie de anchetă, de preferat sub forma unui tribunal condus de un magistrat. Deși procedul va avea loc cu ușile închise totuși concluziile tribunalului vor trebui date publicității".

"Apoi, chiar dacă serviciile secrete au fost sau nu implicate, Guvernul ar trebui să facă demersurile necesare pentru ca atât M.I. 5 cât și M.I. 6 să fie subordonate unei comisii parlamentare. Întreaga opinie publică are dreptul să știe că, atât activitatea, cât și bugetul alocat pentru M.I. 5 și M.I. 6, sunt supuse controlului parlamentar. Chiar și aceste instituții nu vor avea decât de câștigat. Fără o astfel de supraveghere, vor continua să rămână ținta unor acuzații similare".

Cel ce apără serviciile de informații, scriu în același cotidian, din aceeași dată, în articolele "Niciodată despre Serviciul Secret al Majestății sale" semnat de Alan Malcher și "Tehnica de orientare accesibilă oricui" semnat de Steve Goggan, ale căror conținuturi se vor reda tot în rezumat:

"Chiar și convorbirile Reginei sunt interceptate, s-a afirmat atunci când au izbucnit controversele cu privire la acuzațiile aduse agenției M.I. 5 - faptul că ar fi înregistrat convorbirea dintre prințul și prințesa de Wales. În ceea ce privește interceptarea și Implicarea M.I. 5 trebuie subliniate foarte clar două aspecte: în primul rând, persoanele ale căror convorbiri telefonice sunt interceptate, nu pot să afle acest lucru decât dacă serviciile de Informații o doresc; în al doilea rând, este de neimaginat ca un serviciu de informații, sau chiar M.I. 5, la care s-au făcut adeseori referiri, să fi putut să lase să îi scape un material atât de 'sensibil' - cum ar fi transcrierea presupusei convorbiri dintre prinț și prințesa de Highgrove".

"Faptul că primul ministru precum și ministrul de interne au negat implicarea serviciilor de informații, a fost preluat și de specialiști din cadrul industriei de informații, precum și de alte persoane care au lucrat alături de serviciile de informații din Irlanda de Nord - unde este poate cel mai puternic centru de supraveghere electronică din Marea Britanie. Concluzia generală a fost că aceste acuzații nu pot fi luate în serios".

"Unii dintre cei direct implicați și-au exprimat îngrijorarea cu privire la faptul că, până și serviciile de informații ar putea fi victimele unor acuzatori sau ale unor indivizi interesați să obțină doar succese pe plan profesional. Au avut loc numeroase manifestări de indignare atunci când aceștia au primit ca sarcină culegerea de informații despre IRA pe continent - o sarcină deosebit de prestigioasă care fusese înainte privilegiul Secției speciale de poliție, precum și al brigăzii antiteroriste".

Așa cum a subliniat un specialist al serviciilor de informații: "Pare foarte ciudat că, odată cu prelucrarea acestor prerogative de la poliție, profesionalismul serviciilor de informații

a fost descompusă în părți care își pune problema dacă nu cumva serviciile de informații au fost în mod intenționat subminate".

"Adevărul este că serviciile secrete de informații au fost criticate adeseori, încă de la crearea lor, în anul 1909, când erau cunoscute sub denumirea de Biroul secret de informații. Fiind o organizație secretă, în rândurile căreia nu se poate intra decât pe bază de racolare, ea este supusă criticilor, tot ceea ce se publică despre activitatea sa, nu face decât să stârneasce 'apetitul' maselor".

"Se pare că singurul motiv pentru care serviciile de informații au fost acuzate de interceptarea casei regale este acela că dețin personalul și echipamentele de specialitate pentru a coordona aceste activități de supraveghere electronică. Cu toate acestea, membrii din industria care produce tehnologie de securitate sunt conștienți de faptul că, oricine poate cumpăra sau folosi cele mai sofisticate echipamente electronice. De asemenea, se știe foarte bine că aceste echipamente pot intercepta convorbirile din interiorul unei camere, convorbirile telefonice, faxurile, computerele și telefoanele mobile. Conform spuselor lucrătorilor din această industrie, echipamentele sunt într-adevăr sofisticate, însă folosirea lor nu necesită neapărat prezența unui specialist în domeniu".

"Firma Hunter Chase Ltd., cu sediul la Londra, printre serviciile căreia este inclusă și "măturarea" sălilor de consiliu (controlarea din punct de vedere tehnico-operativ), a birourilor și reședințelor particulare de microfoane ascunse, a găsit în nenumărate ocazii astfel de dispozitive în interiorul unor încăperi cu regim strict de securitate. Conform afirmațiilor făcute de Hunter Chase, în Marea Britanie, anual, se cheltuiesc mai mult de 4 milioane lire pentru achiziționarea echipamentelor electronice de supraveghere. Una dintre companii, al cărei nume este preferabil să nu fie menționat, a cheltuit lunar circa 12000 lire, pentru a face reclamă echipamentelor sale".

"Keith Stowell, care a lucrat mai mult de 25 de ani în domeniul investigațiilor secrete, a afirmat că oricine are acces în încăperea respectivă poate introduce tehnică de ascultare doar în câteva secunde. Cei care cunosc modul de lucru al Serviciului de Informații Britanic sunt în unanimitate de acord că tot ceea ce apare scris despre el atrage fără îndoială atenția, datorită puținelor

cunoștințe despre activitatea sa".

"Cel mai familiarizați cu 'universul' Serviciului Britanic de Informații sunt de părere că Stella Remington, care a fost de curând numită în funcția de director general al serviciilor de informații, ar comite practic un act de sinucidere profesională dacă ar ignora procedeele de supraveghere prin interceptare, mai ales într-un moment în care sunt aduse cu regularitate critici modului în care serviciile de informații ripostează față de campania IRA".

Dave Mullings, care a lucrat în domeniul culegerii de informații, în Irlanda de Nord, pe o perioadă de doi ani și a văzut cum se efectuează supravegherea electronică acolo, este de neclintit în convingerile sale: "dacă serviciile de informații ar dori să își arate 'măiestria' în supravegherea familiei regale, nimeni nu ar putea să o facă mai bine".

Probabil că el nu face însă decât să exprime cu voce tare părerea, larg răspândită în rândul experților, atunci când se referă la așa-zisa înregistrare a convorbirii dintre prințul și prințesa de Wales: "Aceasta este 'opera' unui individ care lucrează pe cont propriu și care și-a dat seama de sumele imense care se obțin din publicarea în presă a unor astfel de înregistrări".

Cotidianul german "Frankfurter Allgemeine Zeitung" bazându-se pe cele publicate de revista londoneză "Sun" în nr. 111 din 14 mai 1993 publică în pagina 9 comentariul "Familia regală era ascultată de ani de zile?" din care redăm, în traducere selectiv: "Numărul de joi al revistei londoneze 'Sun', dă asigurări privind autenticitatea conținutului convorbirii publicate în același timp menționând că Serviciul Secret interceptează pe toți membrii familiei regale ...".

"Revista 'Sun' a relatat că Serviciul Secret M.I. 5 interceptează de aproape 10 ani de zile convorbirile oricărui membru aparținând cercului intim al familiei regale. Măsura are la bază motive de securitate, dorința de a proteja familia regală...".

"Tehnica folosită pentru interceptarea convorbirilor prințului și prințesei de Wales este simplă, se poate procura relativ ușor și la prețuri accesibile în toate magazinele de specialitate din țară" - spune ziaristul Steve Boggan.

"Există o întreagă gamă de produse electronice începând cu emițătoare simple, la prețuri de aproximativ 20 lire, până la monitorizare nedetectabile în infraroșu al căror preț ajunge până la

1000 lire".

"Este posibil ca așa-zișii lucrători care au înregistrat convorbirea să fi utilizat echipamente profesionale de interceptare, cu înaltă fidelitate sau așa cum au sugerat unii experți, magnefoane care pot fi activate prin vocea umană".

"Nimic mai simplu decât organizarea unei astfel de operațiuni de supraveghere", a afirmat Richard Ludlum, directorul general al Centrului pentru interceptarea comunicațiilor din Berkahire, Ascot.

"Se poate utiliza orice fel de tehnică, începând cu un emițător conectat la o linie telefonică - prin care se poate intercepta convorbirea sau se poate auzi foarte clar tot ceea ce se petrece într-o încăpăre, folosind echipamente laser care detectează vibrațiile, din rețeaua cristalină a sticlei, determinate de vocea umană".

"Întreaga gamă de produse include printre altele, mijloacele de interceptare introduse în stilouri, calculatoare de buzunar și în alte <<jucării practice>>".

"Interceptarea pe termen lung se poate realiza introducând un microfon (nota autorului: un microemițător) în interiorul rețelei de alimentare care furnizează energie electrică".

"Majoritatea dispozitivelor de interceptare prezintă două dezavantaje: capacitatea limitată a surselor de energie electrică precum și distanța la care pot transmite, către ascultător care, cu ajutorul unui aparat de radio obișnuit, intră pe frecvența pe care a fost fixat dispozitivul de ascultare".

"Unul dintre mijloacele preferate de interceptare este 'microfonul nelimitat' care poate fi camuflat în interiorul unui aparat telefonic, alimentându-se chiar de la sursa acestuia". (A se compara cu ce s-a spus în prezenta lucrare despre sistemul "infinity", de la Capitolul al V-lea.)

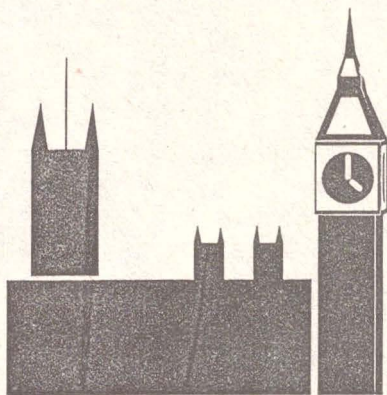
"Avantajul acestui dispozitiv este acela că permite ca interceptarea să poată fi realizată din orice colț al lumii. Nu trebuie decât să formați numărul de telefon al obiectivului, iar în momentul în care acesta răspunde, pretextați că ați format greșit. Chiar dacă acesta închide, ascultarea d-voastră funcționează încă".

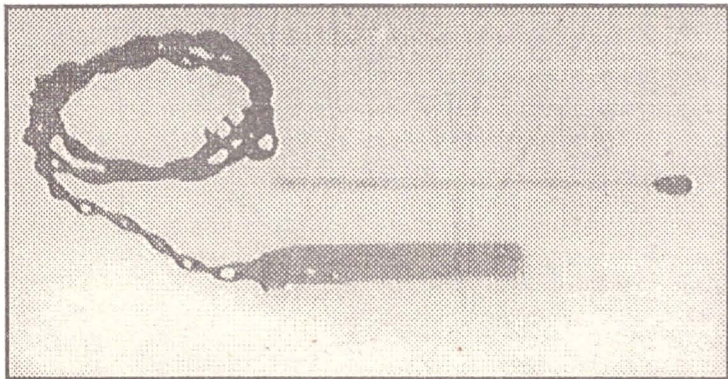
(Nota autorului: Toate afirmațiile privind implicarea serviciilor secrete engleze în interceptarea convorbirilor telefonice ale prințului Charles și ale prințesei Diana, precum și aprecierile făcute asupra aparaturii pretabilă să fie folosită în acest scop, aparțin ziariștilor englezi sau persoanelor citate de aceștia).

*

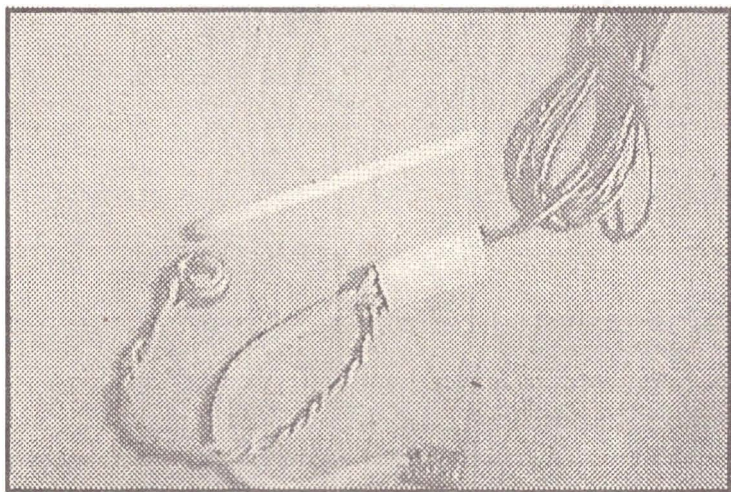
* *

Cititorii care sunt interesați în aceste probleme referitoare la scandalurile produse în urma descoperirii tehnicilor de interceptare pot găsi prezentat în anexa a V-a un alt caz de mare amploare, recent mediatizat în presa spaniolă.

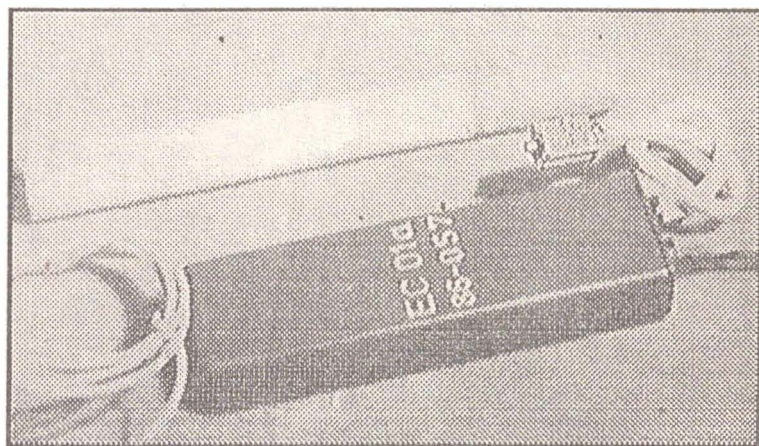
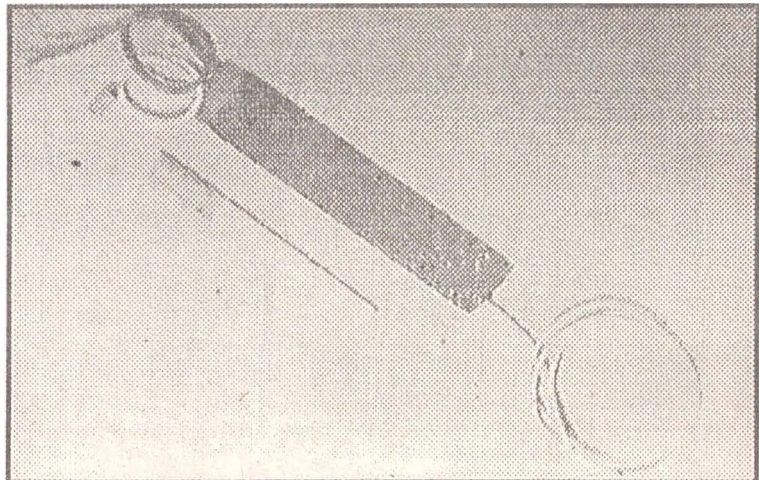




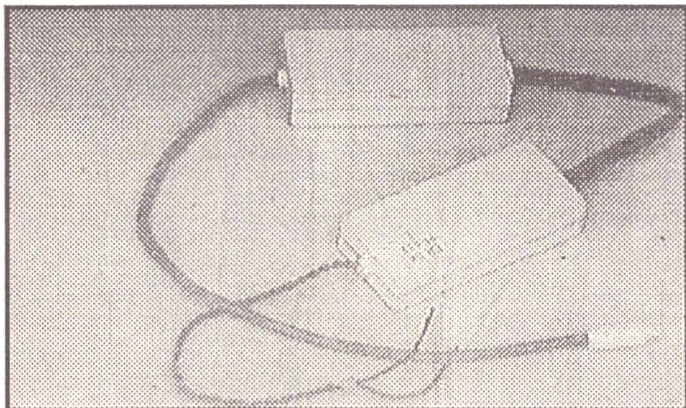
Amplificator cu microfon ceramic incorporat.
Dispozitiv de interceptare cu fir.



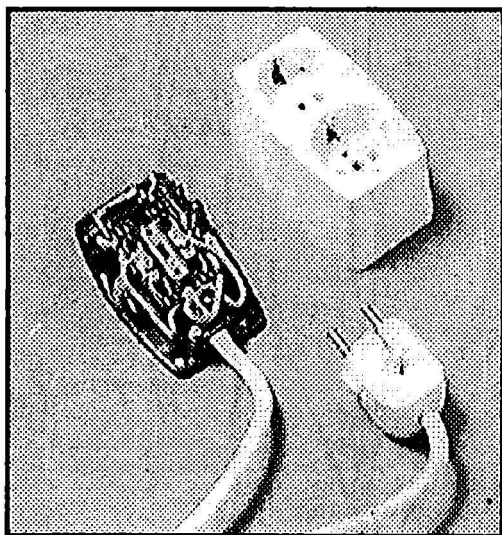
Microemittor cu microfon, bateria de alimentare
si antena monofilara.



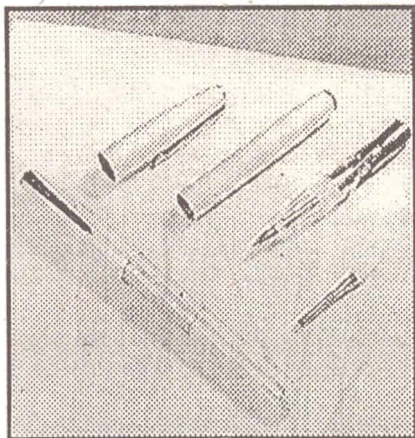
Doua tipuri de emitatoare cu transmisie codificata



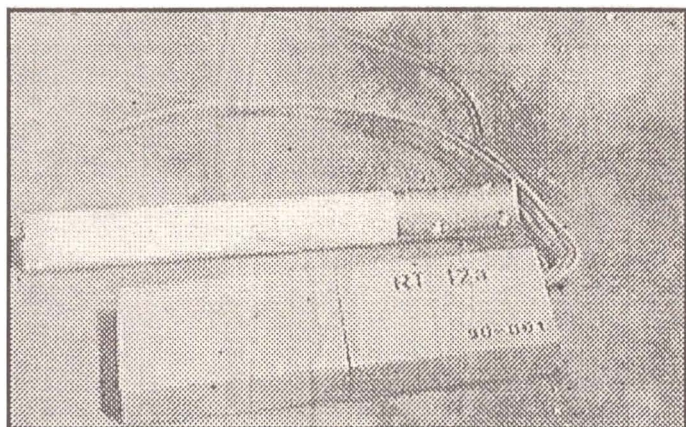
Emilator cu redresor si functionare la retea electrica.



Microemilator alimentat de la retea electrica, mascat intr-un cablu prelungitor.



Microemitor cu baterie electrica
mascad intr-un stilou.



Receptor de telecomanda pentru primirea comenzilor
de pornire si oprire a emilatorului.

CAPITOLUL IX

INTERCEPTAREA PRIN FOLOSIREA SISTEMELOR DIRECȚIONALE OPTICE - LASERI

* S-au tratat la început amplificatoarele de frecvență vocală, s-au prezentat apoi emițătoarele cu curenți purtători împreună cu receptoarele de foarte joasă frecvență sau de joasă frecvență din domeniile de 30 - 300KHz, s-au descris emițătoarele și receptoarele de unde metrice (VHF) 30 - 300MHz, ajungându-se apoi la modul cum se folosesc, în interceptare, fasciculele de microunde și în prezent suntem în fața energiei luminoase din domeniul infraroșu-vizibil-ultraviolet peste 1000 GHz, încât putem afirma că aproape întreg spectrul de frecvență are aplicații în probleme de interceptare și contramăsuri de protecție.

•

* *

Există două tipuri principale de mijloace care folosesc fasciculele de energie luminoasă. În primul rând sunt led-urile sau diodele emițătoare de lumină atât în domeniul infraroșu cât și al energiei luminoase vizibile și în al doilea rând faimoasele lasere. Primele sunt destul de mici, robuste și s-au folosit la început pentru afișare (ceasuri digitale, calculatoare) până ce cristalele lichide le-au luat locul.

Led-ul produce un fascicul energetic destul de larg care, spre deosebire de laser, se dispersează repede cu distanța. Din acest motiv led-ul nu se folosește pe scară largă în interceptare ci îndeosebi în comunicații la mică distanță pentru a rezolva, pe lângă alte probleme și unele legături de spionaj.

În "Science et vie" găsim păreri care apreciază aceste dispozitive de interceptare, și sub titlul "Interceptările luminoase", arată:

"Ultimul născut dintre aparatele destinate să capteze clandestin conversațiile este receptorul de micro-infraroșii. Iată două modele fabricate de Creiec Electronique, o societate

specializată în interceptări și mijloace de protecție. Cum funcționează ele ? Este suficient să disimulăm în încăperea 'spionată' un microemittător, pentru care există astăzi versiuni miniaturizate capabile să capteze o conversație pe o rază de 10 - 15 m. In loc să traducă sunetul în frecvențe radioelectronice, ca majoritatea microemittătoarelor, el trimite un fascicol luminos infraroșu, în gama 800 - 1000 nanometri și deci invizibil cu ochiul liber. Acest fascicol alimentat de o baterie de 9 V sau la rețea, este modulat de către un oscilator. Singura precauție este să vegheai ca minusculul orificiu pe unde iese lumina să fie îndreptat către receptor. Acesta cuprinde o lunetă de vizare (partea superioară a receptorului) care permite reperarea axului diodei de emisie. Luneta inferioară captează fascicolul infraroșu, îl demodulează și îl reconvertește în unde sonore care sunt transmise la un amplificator înainte de a ajunge la casca de ascultare. De asemenea, se poate folosi un receptor parabolic cu un aspect mai puțin amenințător decât primul și cerând mai puțină precizie pentru recuperarea semnalului luminos: acest material este totuși mai bine adaptat la întuneric decât la lumină, în timpul zilei el primind prea multe semnale-parazite. Aceste două aparate pot să servească și la interceptările telefonice, dacă microfonul este cuplat la un adaptor legat la telefonul persoanei <<spionate>>".

Totuși, de fiecare dată când se naște un nou tip de interceptare, apar rapid pe piață și mijloacele de anihilare a lui. Astfel, detectorul CRE 302 localizează orice emisie de infraroșu pe o rază de 1 - 10 m, ceea ce se traduce printr-un semnal sonor în casca persoanei "spionate", sau, într-o altă versiune printr-o pată pe ecran.

Deși prezenta lucrare are un capitol special ce tratează problema comunicării și recepționării datelor de spionaj, bazate pe mijloace tehnice, cele care folosesc energia luminoasă vor fi tratate aici pentru că, diodele emittătoare și laserii sunt elemente principale ale acestor mijloace de transmisiuni. Un led este cuplat cu un banal microfon, sursă de alimentare și un modulator. Tensiunea produsă de microfon, după ce este amplificată, produce modularea luminii generate de led sau, după caz, de laser. Fascicolul modulat poate fi detectat la recepție de un dispozitiv optic sensibil și refăcut semnalul.

Toată construcția se maschează într-un aparat de forma

celui de filmat sau a unei video-camere cu care se poate 'ochi' locul unde trebuie să transmitem (fereastra unui apartament, a unei camere de hotel etc.) care bineînțeles trebuie să se afle la vedere directă. Dacă instalația este bine realizată, detectarea acestor sisteme, în cadrul contramăsurilor, este extrem de dificilă, dacă nu imposibilă. Dispozitivele semiconductoare care generează fascicolul de energie în infraroșu și în cel vizibil, ca și detectoarele cu celulă foto-electrică, din componența receptoarelor sunt foarte ușor de procurat.

Se înțelege că, datorită faptului că legătura nu poate fi realizată așa cum s-a mai spus decât între două puncte care se văd între ele, (fără obstacole), iar în condițiile folosirii led-ului în loc de laser, fascicolul se dispersează rapid, aplicațiile în acest domeniu sunt destul de limitate și numai în scopuri speciale.

Laser - raza morții dar și arma interceptării

Despre laser s-a scris enorm atât în articole și cărți științifice, de popularizare, de aplicații în diverse domenii, dar și în termeni bombastici ca raza morții, arma viitorului care perforază blindajele tancurilor, care distruge avioane și rachete în zbor, principala armă din programul războiului stelelor. Nu există film de science fiction sau de super acțiune în care să nu vedem laserul în roluri nefaste, malefice sau cel puțin mistero-fanteziste.

Marele public n-a înțeles natura laserului, conceptul respectiv și, în imaginea despre acesta, este un amestec între real și fantastic, între admirație și frică.

Laserul (Light Amplification by Stimulated Emission of Radiation), în traducere: amplificarea luminii prin emisia stimulată a radiației, cum este definit în dicționare tehnice, este un dispozitiv de generare sau de amplificare a undelor electromagnetice din domeniul infraroșu, vizibil pe baza efectului de emisie stimulată a radiației. Dacă emisia stimulată este datorată unei radiații exterioare, spunem că laserul funcționează ca amplificator cuantic de radiație iar dacă emisia stimulată este declanșată de primii fotoni emiși din cavitatea rezonantă a laserului este un generator cuantic.

Primul generator cuantic de radiație luminoasă a fost

construit în 1960, de către fizicianul american Theodore Harold Maiman. Este vorba de un laser cu cristal de rubin care produce o lumină roșie. Trebuie să spunem că, spre cinstea fizicienilor noștri, numai peste trei ani (1963) un colectiv, condus de prof. I. Agârbiceanu la I.F.A. construia primul laser românesc.

Laserul este format dintr-un mediu activ (exemplu cristal de rubin), o cavitate rezonantă și o lampă de pompă care, în fond, este un tub cu descărcări în gaze. Aceasta din urmă realizează o excitare a atomilor, moleculelor și ionilor mediului activ prin iradlare cu radiații de o anumită lungime de undă.

Emisia cuantică de lumină are loc în urma tranzițiilor secundare ale atomilor substanței active folosite, produse prin rezonanță de către radiația secundară.

În funcție de mediul activ folosit, există laseri cu solid, cu semiconductori și cu gaz (neon, bioxid de carbon, azot și heliu), acesta din urmă aflat într-un tub de descărcare. Cu bioxidul de carbon s-au obținut cele mai mari puteri în impulsuri (10 KW).

Laserul emite un fascicol îngust, permițând concentrarea energiei pe o suprafață extrem de mică. Lumina produsă de laser este o radiație coerentă, de mare puritate spectrală, de aceeași lungime de undă și diferență de fază.

Spectrul radiației s-a extins permanent, de la infraroșu, vizibil și terminând cu radiația X. Puține invenții au găsit atâtea aplicații în domenii așa de variate ale științei, tehnologiei, medicinei etc., ca laserul.

Acesta a dus la apariția holografiei; cu el se măsoară vibrații în construcții de mașini, se fac analize spectrale în chimie, se prelucreză materiale în metalurgie, se fac teleghidări și măsurători geodezice, este suport în telecomunicații, bisturiu în medicină, cu care se fac cele mai delicate operații chirurgicale, este folosit în industria de armament.

Despre acestea s-au scris și se vor mai scrie, dar pe noi ne interesează o aplicație particulară și anume cea a interceptării convorbirilor.

Cititorii care au urmărit o serie de filme polițiste au remarcat desigur, scene în care detectivii, situați într-o mașină echipată special, au putut să audă, prin intermediul unei raze laser, convorbirile între persoane aflate într-o cameră situată la câțiva zeci de metri de mașină. Această aplicație inedită a laserului se bazează pe proprietatea radiației laser de a rămâne

concentrată, sub forma unui fascicol îngust, chiar după parcurgerea unei distanțe apreciabile. Principiul fizic utilizat este următorul: un emițător laser proiectează de la distanță, pe geamul încăperii care prezintă interes un fascicol laser. La suprafața geamului, o parte din fascicol este reflectată conform legilor opticii (unghiul de incidență este egal cu unghiul de reflexie). Unda reflectată este captată de un receptor prevăzut cu o celulă fotoelectrică. Sub acțiunea sunetelor din încăperea, geamul vibrează. Deși amplitudinea vibrației este foarte mică, ea este suficientă pentru a produce deviația fascicolului reflectat, care nu mai ajunge astfel în întregime la receptor, ci variabil, funcție de vibrațiile geamului. Rezultă astfel o modulație a puterii optice recepționate, în ritmul sunetului din încăperea (fig. 7).

La receptor modulația optică este sesizată de foto-detector, care o transformă în semnal electric. Acesta este apoi amplificat convenabil.

S-ar părea, la prima vedere, că aceste echipamente cu laser, pentru ascultarea de la distanță a convorbirilor, reprezintă echipamentele ideale în domeniu, deoarece nu este necesară instalarea vreunui dispozitiv electronic în încăperea vizată.

În realitate, alinierea emițătorului și a receptorului nu este o problemă simplă. Ne imaginăm dificultatea de a 'capta' la distanță un fascicol de câțiva milimetri. Atunci când condițiile permit se utilizează la început laser în domeniul vizibil și, după captarea razei reflectate se înlocuiește cu cel în infraroșu.

Pe de altă parte, eficacitatea acestui gen de echipament poate fi anihilată cu ușurință prin instalarea, de exemplu, a unor jaluzele prin care raza laser nu penetrează sau dă unghiuri de reflectare greu de controlat. Cel mai mare dușman al folosirii laserului în interceptări clandestine este zgomotul, în special cel provocat de trafic, de vibrațiile clădirilor, de cel al agenților casnici care acționează și ele asupra geamului.

În literatura de specialitate, prin prezentarea unor referate asupra problemei, se arată că, pentru a elimina aceste inconveniente, s-au adus unele îmbunătățiri tehnologice, astfel ca raza laser să fie îndreptată, prin ferestre, asupra unui obiect care este mult mai izolat din punct de vedere al zgomotelor exterioare. Pentru a înlătura și greutatea captării unde reflectate, greu de depistat, se emite ideea că ținta care se montează în cameră poate fi vizual transparentă dar opacă pentru fascicolul laser din

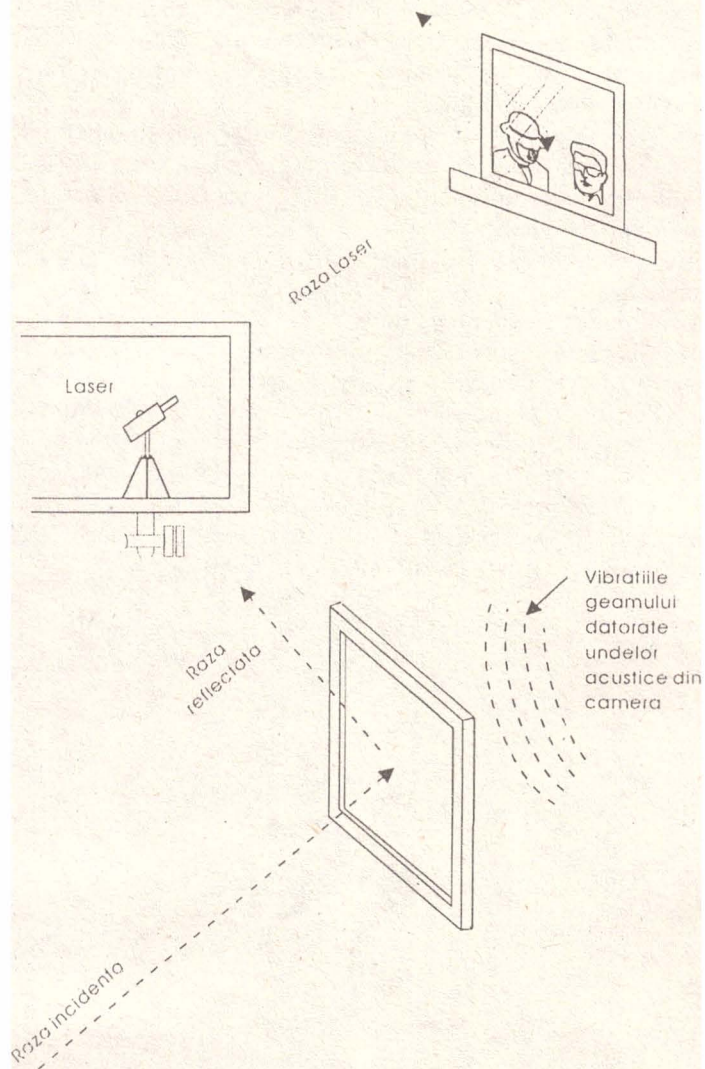


Fig.7. Interceptare cu laser

afara spectrului vizibil. Acest obiect care este un reflector bidimensional poate fi instalat în așa fel încât să reflecte fascicolul laser exact în direcția incidente. Aceste reflectoare sunt constituite dintr-o membrană vibratorie, cu acces optic la unda laser și sonor la discuțiile din zona supravegheată și pot avea un diametru de câțiva cm.

Pentru specialiști spunem că în aceste situații modulația laserului se bazează pe efectul Doppler-Fizeau și este de frecvență, spre deosebire de cea din cazul undei reflectate, care era de amplitudine.

În concluzie, din ceea ce se cunoaște până în prezent, laserul nu este un mijloc eficient, în special din punct de vedere al costului, cu excepția situațiilor când nevoia de informații este atât de mare, încât acesta nu mai contează. Deși laserii sunt destul de ușor disponibili nu există dovezi serioase, credibile, că ar exista sisteme practice de culegere a informațiilor prin aceste metode, dar trebuie să recunoaștem că și cunoașterea în acest domeniu de aplicații este limitată și există o lipsă acută de informații. Poate că aceste date n-au străbătut încă barajul, pe care marile servicii de informații îl pun, pentru ca ceea ce folosesc să devină bun public abia după foarte mulți ani.



CAPITOLUL X

INTERCEPTAREA INFORMAȚIILOR NEAUDITIVE DIN SISTEMELE DE COMUNICAȚII DE DATE

Până în prezent ne-am referit la interceptarea semnalelor vocale din convorbiri ce se poartă cu ajutorul telefoanelor, direct din încăperi sau în aer liber, dar acestea vehiculează un număr limitat de informații. Comunicațiile om-mașină, mașină-mașină, dintre dispozitivul de captare și vizualizare a imaginilor au o densitate mai mare de conținut al informațiilor. Ne propunem să arătăm în acest capitol unde sunt vulnerabile aceste comunicații, fără să insistăm asupra datelor de detaliu ale aparaturii necesare pentru această interceptare, deoarece interesul pentru ele este strict limitat la grupuri de specialiști, la cei care lucrează în domeniu.

*

* *

Multe canale de comunicații se reunesc într-un fascicol hertzian de microunde iar energia se transmite de la releu la releu. Acestea au drept antenă 'pălării' asemănătoare celor folosite în recepția sateliților și pe care le vedem pe clădirea Palatului Telefoanelor din Calea Victoriei, pe cea a Televiziunii și pe toate construcțiile, unde se găsesc radiorelee (exemplu: la intrarea în orașul Slatina, Morărești - pe dealul Negru, Cerbu - jud. Gorj și foarte multe altele). Interceptarea efectivă a acestor transmisii se poate face cu un radioreceptor, pe frecvența adecvată (450 Hz, 900 MHz sau mai mare), dar plasat în raza energiei transmise.

Cititorii își aduc aminte ce acuzații reciproce s-au adus între sovietici și americani, reproșându-și că s-ar ocupa de interceptarea comunicărilor prin microunde, folosind pentru aceasta pozițiile strategice ale ambasadelor, consulatelor, agențiilor economice și locuințelor lor care s-ar afla pe traseele dintre radiorelee. Astfel, americanii spuneau că sovieticii fac acest lucru în Washington și California și invers în Moscova.

Realitatea este că, informații foarte importante se pare că a obținut C.I.A. din interceptarea, cu mulți ani în urmă, a convorbirilor guvernamentale sovietice, până la cifrarea lor, interceptând stațiile centrale și radioreleele pentru comunicații mobile din capitala fostei U.R.S.S.

Captarea transmisiilor din fascicolul de microunde nu asigură sursa de informații audio direct accesibilă, întrucât necesită o amplă prelucrare pentru separarea canalelor de comunicații folosite.

Parcă, pentru a îngreuna interceptarea, progresul științific și tehnologic în domeniul comunicațiilor a dus la folosirea undelor milimetrice care se propagă prin cabluri subterane, ce sunt mai puțin susceptibile de a fi interceptate. O altă tehnologie pentru comunicații grupate, cu zeci de mii de canale de date, transmise simultan, face apel la fibrele optice și energia luminoasă. O singură fibră de sticlă poate înlocui multe canale pe fir, datorită capacității mari de transport a semnalelor. Ne imaginăm că, de data aceasta, sunt greutăți și mai mari de interceptare atât datorită dificultăților de cuplare la fibra de sticlă și, în special, în a identifica ceea ce interesează.

Vulnerabilitatea calculatoarelor

Datorită vastității extinderii pe care au luat-o în prezent rețelele și sistemele de calculatoare care leagă instituții guvernamentale, întreprinderi industriale, comerciale și în special bancare, nu se putea ca acestea să nu devină obiectiv al interceptării, pentru că în ele se stochează și se manipulează informații deosebite, ca tranzacții de credite, de bursă, de date arhivistice etc. Toți cei care au vizionat filmul serial italian "Caracatița" au reținut uriasa cantitate de date referitoare la transferuri de capital care se manipulează prin calculatoare și ce bătaie se dă pentru a fi descoperită.

Presa a publicat în permanență date privind celebre furturi și deturnări de fonduri, efectuate de diverși cetățeni particulari, cu precădere tineri, cu aplicații și cunoștințe în informatică și calculatoare. În manipularea și supravegherea electronică a calculatoarelor se disting trei stadii: interceptația, amestecul și

falsul. În stadiul de interceptare, terminalul de date al unui beneficiar legal este conectat printr-o derivație sau cu un emițător, asemănător cu cel al telefonului și prin care se vor transmite datele, la un post de ascultare.

Se urmărește fie schimbul de date introduse și răspunsurile computerului, fie doar preludiul unei strategii de manipulare, necesitând cunoașterea funcționării sistemului, numere de identitate, tehnica de bilanț automat a terminalului ales ca obiectiv.

Prin amestec în funcționarea normală a calculatorului se înțelege negarea dreptului beneficiarului legitim de a dispune de serviciile corecte ale computerului. Aceasta include înregistrarea de mesaje false sau modificarea celor transmise de beneficiar. Pentru acest gen de activități, de interes special al instituțiilor bancare și burselor de valori, este nevoie de interceptarea liniilor unui terminal al calculatorului principal și folosirea unui alt terminal sau minicomputer cu claviatură care este programat să comunice cu computerul principal.

Aparatura necesară acestui "amestec" așa cum l-am descris costă în jur de 5 - 7000 dolari S.U.A.

Dacă se dorește numai obținerea de informații, operațiile se opresc aici, iar dacă nu, se trece la cea de-a treia fază, privind derutarea computerului și realizarea falsului. Este o operație lungă, de acumulări de date, de identificare a interceptorului cu un client de drept care va putea folosi computerul ca un operator legal, manipulând dosare de credit, date de conturi bancare, cu pericole minime de depistare.

Trebuie spus că există o preocupare serioasă din partea multor factori, în special a constructorilor de calculatoare, pentru asigurarea securității acestora, prin cifrarea și descifrarea datelor manipulate, coduri diferite de acces la calculator funcție de banca de date solicitată, timpi de programare pentru fiecare terminal etc. Pentru unele bănci de date deosebit de secrete, stocate în calculator, se iau măsuri speciale pentru a verifica și reduce accesul la ele.

Telexurile și telefaxurile se interceptează la fel ca telefoanele

Dintre echipamentele de transmis și prelucrat date, cele mai folosite sunt telexurile, telefaxurile, imprimantele terminale, mașinile de scris electrice etc. Toate acestea pot fi interceptate, în primul rând dacă există acces la linia de legătură ce conectează, spre exemplu, telexurile la rețeaua care poartă același nume. Se înțelege că, având o derivație și un aparat similar, tot ce transmite sau recepționează telexul supravegheat va fi prins și de cel introdus pe rețea în mod clandestin. Branșarea pentru interceptare se poate face atât în serie, cât și în paralel, pe circuitul telex. Pentru a evita folosirea unui aparat telex pentru interceptare, deoarece se consumă hârtie și acesta are o uzură mare a pieselor în mișcare, se folosesc magnetofona drept mijloace de înregistrare a mesajelor interceptate. Pentru aceasta, semnalele telex interceptate modulează o frecvență din banda audio, care apoi este înregistrată. Cu dispozitive electronice similare, porțiunile interesante din înregistrare pot fi citite, la cerere, pe un telex.

Pentru că în ultimul timp s-au răspândit telefaxurile și toate societățile trimit și primesc faxuri, trebuie să spunem că și pentru acestea s-a realizat aparatură de interceptare care se montează la fel ca și în cazul interceptării telex doar că branșarea se face pe linie telefonică. Această aparatură poate intercepta simultan mai multe linii telefax, poate stoca și memora datele de pe sute de pagini format A₄ și le poate transmite la un calculator sau la orice post telefonic dotat cu aparatură de memorare sau de citire.

Interceptarea faxurilor este ușurată și de faptul că utilizatorii nu știu să folosească unele facilități create de constructorii acestora, prin dotarea unor tipuri de telefaxuri moderne cu coduri de recunoaștere, care îngreunează accesul la ele și deci și la interceptare.

"Science et vie" în articolul consacrat interceptărilor din Hexagone al numărului din iunie 1992 confirmă aceste date sub titlul: "*Faxurile sunt ascultate*". Redăm traducerea:

"Acest controlor portabil, comercializat de către Confrexport, permite, de exemplu, să se înregistreze toate faxurile

unui concurent. Este suficient să se branșeze un fir, racordat la acest aparat, pe cablul abonatului spionat și telecopia pornește pe rețeaua telefonică. Această derivație poate fi făcută în orice punct pe cablu, atât în repartitor cât și la o distanță de 2 km".

Cea mai bună protecție împotriva interceptării telex și a celei telefonice este folosirea aparaturii de cifrare. Se pot proiecta și s-au și construit pentru scopuri speciale aparate de cifrat telex cu bandă perforată aleatoare care sunt nedecriptibile. Deși au putere de cifrare maximă, dat fiind greutatea organizatorice necesare funcționării legăturilor (confecționarea benzii aleatoare cu instalații speciale și transmiterea lor la toți abonații) nu sunt fabricate, așa cum am mai spus decât pentru rezolvarea unor cazuri deosebite.

S-au construit și răspândit foarte multe aparate de cifrare cu generator intern pseudo-aleator cu chei de bază memorate, cu cheile de mesaj cu perioadă foarte mare și care poate funcționa cu 50, 75, 100 bauds.

Dar aceste aparate pot fi interceptate nu numai prin derivațiile de pe liniile pe care funcționează, ci prezintă inconvenientul radiațiilor care, captate și prelucrate, pot da foarte multe informații, care să ducă la refacerea mesajului în clar.

Radiațiile parazite sunt prin natura lor, acustice, magnetice și de radiofrecvență. În funcție de acest lucru, ele pot fi captate cu microfoane, bobine și antene, direct de la sursă sau din apropiere. Se fac analize complexe ale multiplelor armonici ale acestor radiații dar costul și complexitatea unei asemenea operații o fac inaccesibilă aproape pentru toți, în afară de câțiva interceptori rafinați. Se constată un slab interes în această direcție, în afară eventual, de partea teoretică a problemei.

Totuși, numai faptul că și tehnic este realizabilă interceptarea, a făcut ca, la toți acești procesori electromecanici să se ia măsuri deosebite. Astfel, s-au înlocuit toate releele cu circuite de comutație electronică cu semiconductori, s-au blindat ori ecranat bobinele, s-au deparazitat contactele și s-au montat filtre pe rețeaua electrică.

CAPITOLUL XI

METODE ȘI MIJLOACE FOTO, CHIMICE ȘI ELECTRONICE PENTRU TRANSMIS INFORMAȚII. SOLUȚII PENTRU DEPISTAREA ACESTORA

Să presupunem că un serviciu de informații dispune de un agent ce acționează într-o altă țară îndepărtată și că obișnuitele contacte personale cu acesta îi sunt îngreunate din diverse motive: fie datorită greutăților de a călători în alte țări, situație care a existat în unele părți ale lumii până la sfârșitul anilor '80 și începutul deceniului următor, fie datorită faptului că, în general, cadrele serviciilor de spionaj sunt filate de contraspionajul țării vizate, fie că este nevoie de contacte și legături foarte dese care nu pot fi rezolvate numai prin cele personale, fie că pot interveni situații speciale: crize, războaie, revoluții, care fac imposibile aceste legături (și tocmai atunci sunt necesare mai multe contacte). Serviciul de informații are nevoie să transmită ordine, sarcini, cerințe și să primească date, informații, iar agentul să știe ce trebuie să întreprindă și să-și valorifice rezultatele activității sale, prin expedierea informațiilor obținute.

Dacă vom trata în această lucrare numai mijloacele tehnice de legături, nu înseamnă că celelalte nu se mai folosesc. Si cele mai importante servicii de spionaj predau și primesc materiale ce conțin informații, rapoarte, sarcini, sub forma unor fotografii, rapoarte etc., în locuri ascunse, care par nevinovate, în așa numitele căsuțe poștale, dar descrierea în detaliu a acestora nu intră în tematica pe care o abordăm.

Ne vom referi în schimb la micropunct, cerneală simpatice (invizibilă), indigouri, la emițătoare de diferite tipuri.

În patru milimetri pătrați o pagină de informații

Prin micropunct înțelegem un procedeu foto, cu ajutorul căruia datele care sunt cuprinse într-o pagină format A₄ sunt transpuse pe o porțiune de film, în suprafață de maximum 4 mm².

Nu, nu este nici o greșeală, o pagină în câțiva mm² de peliculă foto și metoda nu este nici măcar nouă, ea se folosește de peste 50 de ani. A fost procedeul principal prin care Allen W. Dulles, șeful serviciului de spionaj american în timpul celui de-al doilea război mondial, cu reședința în Elveția, își primea rapoartele secrete de la agenții săi.

Se folosește, de regulă, de la agent către centrala de spionaj și foarte rar, invers. Fiind la îndemâna primului, procedeul de fabricare și trimitere trebuie să fie simplu, ușor de învățat după un anumit instructaj și să nu necesite scule și dispozitive compromițătoare, în caz că sunt descoperite.

Astfel, un aparat foto normal și un mic colț dintr-o cameră, chichinetă, hol, baie, căreia să i se asigure la dorință, obscuritatea, apă și tot ce este necesar dezvoltării și realizării fotografiilor, nu pot constitui probe compromițătoare pentru un agent. Sunt foarte mulți cere au această pasiune și sunt fotografi amatori. Interesant este să se prezinte tehnologia de fabricare a micropunctului. Pagina care conține informațiile este, la început, fotografiată cu aparatură clasică, pe un film normal, în dimensiunile standard (36 x 24 mm). Acesta este, la rândul lui, micșorat cu ajutorul unui obiectiv foto (practic o lentilă) și redus la dimensiunea de 2 x 2 mm, după toate regulile artei fotografice dar cu modalități empirice. Singura piesă compromițătoare pentru agent, în caz că este găsită, este micul obiectiv care nu-și are rostul să facă parte din dotarea unui laborator, al unui fotograf amator. De aceea această piesă este montată mascat în diferite obiecte (țigaretă, stilou etc.) și păstrată separat.

Sigur există și procedee foto automate (ne-empirice) cu aparatură chiar sofisticată, asemănătoare celei care microfizează cu mare randament documente, cărți și alte lucrări pentru arhive naționale, biblioteci, servicii de documentare și transpunere pe peliculă foto de dimensiuni de la 10 ori (iar ca suprafață de 100 ori) mai mari ca cele ale micropunctului.

Astfel de aparatură adaptată scopului propus, poate fi folosită de Serviciul de Informații (Centrală) care realizează foarte multe micropuncte dar în nici un caz nu se justifică în locuința unui agent, decât dacă, pentru acoperire, acesta practică oficial, ca sarcină de serviciu, activitatea de microfizare. Microfilmul obținut, așa cum am arătat, după dezvoltare și subțiere (înlăturarea suportului de rezistență care nu conține emulsia foto),

este plasat într-o ravisă și expedit la destinația, chiar prin poștă. Pentru a-l ascunde, nu este nevoie decât de un bisturiu sau o lamă ca să cresteza locul, pe pagina unde-l vom planta și o seringă, cu care vom lpi, cu clei special, tăietura executată. Pe pagina unei reviste se pot găsi zeci de locuri unde se pot ascunde "microdots", cum sunt numite micropunctele în literatura de specialitate.

Așa se petrec, în mere, operațiunile cu realizarea și expedierea lor. Lucrarea n-a intrat în detalii, pentru că nu ne-am propus lecții de instruire ci numai o prezentare succintă, astfel ca cititorul să-și formeze o idee veridică, clară, asupra metodei, a performanțelor obținute și să poată discerne singur ceea ce este posibil, real, ca se folosește și ce este fabulație, pentru că în domeniul acesta, pe lângă lucruri și fapte reale, s-au prezentat și fapte care nu au nici o legătură cu realitatea.

Metoda asigură securitatea agentului, mai ales dacă acesta realizează o trimitere poștală numai cu destinatar, fără să treacă expeditorul sau dacă-l scrie, acesta să fie fictiv. Astfel, chiar dacă micropunctul este depistat, nu înseamnă că se deține identitatea agentului, a expeditorului real.

Referindu-ne la operația căutării și depistării unui micropunct într-o revistă voluminoasă, cum este "Paris Match" spre exemplu, sau într-o carte, trebuie să spunem că operațiunea necesită o muncă uriașă, de cele mai multe ori sortită eșecului. Numai dacă sunt date sigure că micropunctul există, se poate încerca depistarea lui, folosind pentru aceasta observarea atentă cu ochiul liber, cu lumina care cade pe pagină sub diferite unghiuri, cu o lupă sau chiar cu microscopul. Alte metode nu se pot imagina și când te gândești că o revistă are zeci de pagini și că se vehiculează prin poștă sute de titluri în zeci de mii de exemplare, ce să cauți ? Trăiască spionajul, vai de contraspionaj!

Există și cerneală invizibilă

Prin transmiterea cu cerneală simpatcă, invizibilă, se înțelege comunicarea prin scris cu ajutorul unor substanțe chimice, pe hârtie albă sau alte suporturi și care nu este lizibilă, fără să se întreprindă alte măsuri suplimentare. Dacă porțiunea

scrisă este însă tratată cu o anumită substanță chimică, numită revelator, scrisul poate fi citit în condiții optime.

Procedeu este cunoscut de mult și folosit de tineri îndrăgostiți, liceeni în scrisorile de dragoste pe care și le trimit sau în jurnalele intime pe care le țin. Cea mai folosită substanță pentru aceste scopuri este zeama de lămâie (acid citric diluat), precum și soluția cu aspirină, dar și multe altele - așa zis - banale.

Sigur că, în probleme de spionaj nu poate fi vorba de așa ceva și se folosesc compuși, ce rezultă dintr-o perfectă cunoaștere a chimiei organice și care nu pot fi evidențiați decât tot cu o substanță complexă.

Cu cât un produs chimic devine lizibil prin reacție de culoare, la cât mai puține substanțe (ideal - una singură - revelator specific), cu atât este mai proprie folosirea lui în această metodă de transmitere de informații. Scrierea cu aceste soluții chimice se face între rândurile completate cu cerneală normală sau în alte porțiuni libere ale unei scrisori (verso unei pagini, porțiunea rămasă pe o pagină care n-a fost scrisă complet cu cerneală obișnuită). Desigur, această transmitere nu se face numai prin hârtia scrisorii și se poate folosi, funcție de situația dată, orice suport pe care se poate scrie (materiale textile).

Ne imaginăm ușor ce înseamnă să se caute și să se depisteze, într-o scrisoare suspectă, aceste comunicări ascunse. Teoretic și practic această operație trebuie să înceapă cu revelatori de grup (ce evidențiază mai multe substanțe) și apoi specifici, care sunt cunoscuți și publicați în diverse lucrări de specialitate sau ca urmare a unor cercetări proprii ale unui serviciu de contraspionaj puternic (nu ne putem imagina că FBI ori SIR, urmașul KGB-ului, nu dispun de laboratoare și cadre, de specialiști necesari).

Din păcate, procedând astfel, hârtia scrisorii sau alt suport este deteriorată și nu mai poate fi trimisă la destinație pentru a nu se afla că acest canal de transmitere a devenit suspect și că materialele respective au fost supuse controlului.

Indigoul este uneori alb

Metoda a fost perfecționată și s-a ajuns la indigoul alb. Este și mult mai comodă, științifică și nu prezintă inconvenientul zgârieturilor pe hârtia albă, produse de instrumentul cu care se

scrie direct pe hârtie cu cerneală invizibilă, care pot fi evidențiate cu iluminare oblică puternică. În noua metodă nu se scrie cu substanță lichidă, ci se folosesc substanțe solide sub formă de pudră, cu care se impregnează, prin presare simplă sau calandrarea suprafeței foi de hârtie (lambele părți, pentru mai multă siguranță). Astfel, am obținut hârtie de "indigo" care apoi se taie în aceleași dimensiuni cu cele ale hârtiei pe care o vom folosi pentru trimiterile de informații. Peste hârtia pe care dorim să scriem invizibil, se așează "indigoul". Deasupra lor, se pune o foaie "nevinovată" pe care se scrie textul dorit, puțin mai apăsător ca de obicei. Substanța chimică din suprafața indigoului pătrunde pe porțiunile apăsate și se depune pe hârtia scrisorii. Se observă că este exact metoda prin care se obțin copii cu ajutorul indigoului obișnuit (de aici și denumirea metodei). Prin procedee de relevare, asemănătoare cu cele din prima metodă (a cernelei simpatice), la destinatar se evidențiază scrisul. Problemele sunt deosebit de complexe pentru a descoperi noi substanțe chimice pentru indigourile cu care să fie dotați și agenți recent recrutați și introduși în rețea. Din motive lesne de înțeles, este bine ca o substanță - indigo să nu fie dată la doi agenți. Substanță nouă se consideră cea care nu răspunde la nici un reactiv din rețeta acestora, cunoscută până la un moment dat. Probleme la fel de grele, dacă nu mult mai dificile, sunt pentru cei ce încearcă să descopere scrisul când nu se cunoaște substanța folosită ca indigou. În această operație, odată tratat materialul suspectat cu un singur reactiv, acesta este practic distrus, ca și în cazul depistării cernelei simpatice și nu mai poate fi nici expediat și nici continuat controlul cu alți reactivi. În literatura de specialitate se arată că pentru astfel de situații, materialul de controlat este supus unui tratament nedistructiv. Acest procedeu este descris în felul următor: peste hârtia suspectă se pune o altă, cu proprietăți asemănătoare sugativei puțin umezită și se presează foarte tare. Dacă pe hârtia controlată există urme de substanțe chimice (altele decât cele din compoziția ei) care au fost imprimate prin apăsare, se vor putea preleva în cantități mici și pe hârtia sugativă. Aceasta din urmă este tăiată în zeci de franjuri și fiecare, sau grupuri dintre ele, alese după anumite criterii, vor fi tratate cu anumiți reactivi. Dacă la reacția cu unul dintre aceștia se observă apariția unor litere sau semne ca urmare a depunerii substanței indigoului, se reia operația cu grijă pe suprafețe din ce în ce mai

mari, apoi pe toate franjurile, cu reactivul la care s-a răspuns. Se înțelege că sunt operații foarte greoaie, ce nu pot fi aplicate la materiale în proporție de masă.

De aceea, pentru a reduce numărul materialelor asupra cărora se acționează chimic, care cere foarte mult timp, este necesar să se facă o preselecție, după cum se deduce și din lecturarea atentă a literaturii de specialitate și anume un control fizic nedistructiv și mult mai rapid, pentru a depista, cu ajutorul unei lumini albe puternice, sub diferite unghiuri de incidență asupra hârtiei controlate, precum și cu lumină ultravioletă de diferite lungimi de undă. Se urmărește identificarea anumitor urme de apăsare și fluorescență, diferite față de cele ale masei hârtiei. Numai cele care devin suspecte la acest control se supun procedurilor chimice de depistare. Transmiterea de informații cu mijloace chimice este foarte comodă și sigură pentru agent. El primește de la "Centrală" carnetul cu indigouri (ca și substanța chimică pentru cerneală), reactivul de probă (fără să știe ce este din punct de vedere chimic) topul de hârtie și plicurile pentru trimiteri.

Siguranța este dată de greutatea enormă în detectarea comunicării numai prin procedee fizice, chimice, optice. Ele sunt folosite pentru completarea sau eliminarea unor suspiciuni existente, claritate comportamentului și activității unei persoane bănuite a fi agent al unui serviciu de informații. Astfel, din punct de vedere al trimiterii informațiilor, o persoană devine suspectă de spionaj-trădare când scrie la aceeași adresă, dar nu primește răspuns (legătură unilaterală), nu completează rubricile cu datele expeditorului, sau prezintă date fictive etc. În istoria modernă a spionajului, se cunosc foarte puține cazuri când căderea unui spion a plecat de la depistarea acestor mijloace foto-chimice de transmis informații, prinderea acestuia datorându-se altor cauze și tabloul integral al activității de spionaj a fost completat cu descoperirea mijloacelor de transmitere a datelor obținute din activitatea sa.

În adevăr, la cei mai mulți dintre agenții serviciilor de spionaj arestați, la percheziție, li s-au găsit materiale pentru transmiterea de informații pe această cale. Publicațiile ce tratează istoria spionajului sunt pline de fotografii în care se prezintă sticlute cu cerneală simpatică și revelatori, carnete cu indigouri, tabele de codificare care au aparținut în special agenților sovietici

capturați în Anglia sau S.U.A. Serviciile de contrainformații române sunt în posesia unor astfel de materiale, care au fost folosite de agenți recrutați de C.I.A. în perioada războiului rece.

O altă țară, fostă socialistă, care înainte a făcut parte din Tratatul de la Varșovia și astăzi este plasată în grupul țărilor de la Visegrad a pus, în anii '70, în aplicare un sistem ingenios de evidență a trimiterilor poștale externe (plecări-sosiri), folosind ordinatoarele și criterii riguroase de selecție, pentru a depista pe cele care sunt pretabile să fie folosite pentru transmișii secrete de informații și care să fie supuse controlului fizico-chimic.

Trebuie spus că deși în toate țările controlul secret al trimiterilor poștale ca și interceptarea convorbirilor telefonice sunt ilegale există multe excepții care le fac practicabile.

Mass-media i-a acordat cenzurii poștale mai puțină "atenție" decât problemei controlului secret al telefoanelor.

Spionii au în dotare emițătoare

Nu se putea ca electronica să nu-și spună cuvântul și în acest domeniu al transmișii informațiilor rezultate din spionaj și aceasta chiar înaintea chimiei și foto-opticii. În practică, se întâlnesc mai multe situații când se folosesc diferite tipuri de mijloace electronice. În primul rând, necesitatea de a transmite la distanțe continentale sau intercontinentale (500 - 5000 km) cum pot fi cele dintre centrală - agent și care necesită anumite tipuri de aparatură, sau de zeci, sute de metri, când se folosesc alte mijloace electronice, cu alte performanțe și caracteristici. Legătura dintre centrală spre agent, pentru distanțe foarte mari, este ușor de realizat și nu pune probleme deosebite. Serviciul de informații închiriază sau folosește propriile sale emițătoare (dacă este vorba de unul de talia C.I.A., S.I.R., S.D.E.C.E. - francez etc.) de unde scurte, așa cum sunt cele folosite de radiodifuziune. Transmisia se face de obicei la viteze normale, cifrat în fonie sau telegrafie. Pentru mai multă siguranță mesajele se repetă și înaintea lor se transmit melodii sau alte semnale de recunoaștere. Cititorii mai în vârstă își amintesc că în timpul celui de-al II-lea război mondial serviciile de informații militare britanice și americane foloseau emițătoarele de radiodifuziune B.B.C. pentru a transmite ordine agenților care acționau în Franța, în teritoriul ocupat. Agentul care

urmează să primească mesajele nu trebuie să aibă decât un receptor de calitate cu extensie de bandă în unde scurte și, eventual, un magnetofon, piese pe care și le poate procura singur și care nu pot constitui probe compromițătoare.

În general, funcționarea receptorului pe o anumită frecvență nu poate fi depistată decât dacă asupra acestuia se iau măsuri speciale, ceea ce înseamnă că posesorul receptorului ridică deja suspiciuni deosebite. Pentru aceasta, în aparatul de recepție se introduce în mod secret un microemittător, care transmite la distanță de câțiva zeci, sau sute de metri semnalele captate de receptor.

Nu așa stau lucrurile când legătura pe cale de emisie-recepție se face în mod invers și anume de la agent la centrală. Acesta nu are posibilitățile unei instituții guvernamentale, el acționează ascuns, nu are la dispoziție emittătoare de mare putere, ci trebuie să folosească aparate de puteri și dimensiuni rezonabile care pot fi păstrate la locuri sigure. Legătura agent-centrală, prin intermediul acestor emittătoare, poate fi de bază sau de rezervă, pentru situații deosebite când alte posibilități (contacte personale, transmițeri cu indigouri și micropuncte) nu există. Deoarece este foarte periculoasă, de regulă, această legătură se folosește doar în cazuri deosebite. Ieșirea în eter poate fi sesizată mai ales când de aceasta se ocupă servicii de contrainformații-radio, de goniometrie, bine înzestrate și dotate cu cadre specializate, respectiv aparatură adecvată.

Aceste emittătoare au o putere de 40 - 100 W și posibilitatea să emită, pe frecvențe foarte multe, în întreaga gamă a undelor scurte, decametrice (3-30 MHz) permițând funcționarea eficientă, atât ziua cât și noaptea, în toate anotimpurile. Este bine cunoscut faptul că pentru asigurarea unei bune legături la distanță mare, mai importantă decât puterea emittătorului este alegerea corectă a frecvenței, funcție de condițiile de propagare existente care, la rândul lor, sunt dependente de anotimpul și în special ora de zi sau noapte la care se emite. În ultimul timp emittătoarele s-au perfecționat, în sensul că necesită foarte puține reglaje care trebuie făcute de operator, în special pentru adaptarea cu antena, restul acordurilor făcându-se automat, odată cu schimbarea frecvenței. Ele dispun de posibilitatea de a transmite foarte rapid (câteva secunde de emisie), au o stabilitate bună în frecvență cu ajutorul cuarțului și sunt dotate cu anexe, pentru cifrarea și

memorarea mesajului. Mărirea vitezei de transmitere s-a realizat în mai multe etape. La început au fost folosite în acest scop dispozitive electromecanice, acționate manual sau cu motoare miniaturale care, asemănător telexului, antrenau și "citeau" hârtia sau filmul perforat, purtătoare de informație.

Odată cu apariția magnetofonelor miniaturale, mesajul se înregistra la o viteză foarte mică (1,2 - 2,4 cm/s) și se transmitea cu o viteză superioară (38 cm/s). Adevăratele performanțe în domeniu au apărut odată cu dezvoltarea tehnicii de calcul și a dispozitivelor de memorare. Mesajele sunt înscrise la viteze reduse și apoi redade cu frecvențe de tact foarte mari, limitate totuși de viteza maximă de transmitere a canalului de comunicații, care în cazul undelor scurte, funcție de foarte mulți parametri, este de câteva sute de impulsuri pe secundă. De regulă, aceste emițătoare transmit 6000 - 7000 caractere pe minut, ceea ce echivalează cu o viteză de circa 500 - 600 impulsuri pe secundă. Aceste performanțe au îngreunat la maxim localizarea lor, fără să ne referim și la posibilitatea de a schimba permanent, cu fiecare nouă emisie, locul de unde se acționează. Ultima perfecționare, la care asistăm recent, este emiterea pe frecvențe diferite, saltul de pe una pe alta făcându-se după un program prestabilit, schimbare greu de depistat de cei ce goniometrează.

Situațiile operative, așa cum am arătat, cer și legături pe distanțe scurte, foarte repede și sigure. Acestea se folosesc pentru trimiterea de informații dintre agenți și reprezentanți acoperiți ai centralei care lucrează chiar în țara de rezidență a agentului.

Legătura se realizează până la maxim 100 - 300 metri de sediul unde lucrează cadrele centralei (ambasadă, consulat etc.). Agentul dispune și se folosește de un emițător de 1-3 W, în banda undelor metrice (30 - 300 MHz), sau poate să emită pe frecvențe și mai mari, cu viteze de transmitere de 3000 impulsuri/secundă și cu posibilitatea să i se confirme automat că mesajul a fost recepționat corect. El se montează într-un autoturism, sau într-o servietă (în aceste variante legătura poate avea loc și în localuri publice (restaurant, cinematograf).

La ora prestabilită, la locul știut, agentul apasă pe un buton și declanșează astfel transmiterea. Mesajul poate fi repetat de câteva ori pentru și mai multă siguranță. Este greu de presupus că o astfel de acțiune rapidă poate fi detectată de către organele tehnice de contraspionaj, decât dacă, în prealabil, s-au luat măsuri

de control permanent al zonei. Si în aceste condiții se poate seșiza o apariție în eter pe o anumită frecvență, dar până la depistarea mașinii din care a fost făcută, și de aici a agentului, mai este încă drum lung de parcurs pentru că acesta a dispărut de la locul acțiunii.

Trebuie spus că până să ajungă la apăsarea pe buton, agentul își pregătește în liniște, acasă, mesajul pe care îl cifrează, înregistrează și îl stochează în memoria aparatului, sau într-un magnetofon anexă.

Aparatura de interceptare folosită pe rețeaua electrică - (așa cum a fost descrisă la Capitolul al VI-lea), cu puține modificări, poate fi întrebuințată și pentru legăturile dintre ofițerii centralei și agenții lor, în locuri propice acestui scop (hoteluri, campinguri etc.) fără să atragă atenția asupra lor.

*

* *

Din cele spuse până aici, se impun anumite concluzii: legătura duplex ideală folosită în situații normale, este cea radio, dintre centrală - agent, folosind emițători puternici, iar invers, cea cu mijloace foto-chimice indigou - micropunct.

În situații de război, când turismul și poșta internațională suferă grave perturbații se înmulțesc emițătoarele pentru transmis la distanță, așa cum au fost cele ale celebrelor rețele Rotte - Kapelle, Sorge, cele care asigurau legătura dintre Berlin - Zurich - Moscova în timpul celui de-al II-lea război mondial și sutele de emițătoare parașutate odată cu grupurile pe care le trimiteau în Franța serviciile de informații engleze.

În timp de pace, chiar în perioada războiului rece, astfel de emițătoare au stat în conservare, ascunse, ieșind la lumină după descoperirea (cu alte mijloace și din alte motive) și capturarea agenților, așa cum s-a întâmplat cu mulți dintre cei ce au aparținut rețelelor sovietice și au fost descoperiți de contraspionajul englez în Marea Britanie.

CAPITOLUL XII

MIJLOACE ȘI DISPOZITIVE OPTICE ȘI ELECTRONICE PENTRU SUPRAVEGHEREA FIZICĂ ȘI ÎNREGISTRAREA IMAGINILOR

În activitatea de contraspionaj este deosebit de important nu numai a afla ceea ce se discută și se transmite, dar să și cunoști ce face, cu cine se întâlnește, ce obiective vizitează subiectul suspect. Pentru documentarea acțiunilor de spionaj și convingerea autorităților judecătorești de vinovăția sau nevinovăția unui învinuit, precum și pentru determinarea spionilor să-și recunoască faptele este necesar ca principalele momente rezultate din supravegherea fizică să fie prinse pe peliculă foto, bandă magnetică sau memorate cu ajutorul circuitelor electronice și vizualizate cu instalații TV.

Aparate și mijloace pentru fotografieri secrete

Primele dispozitive care se folosesc și astăzi sunt foto-aparatele clasice, dar cu obiective speciale și cu armare automată, cu arc sau motor, pentru a nu mai fi nevoie să se armeze după realizarea fiecărei fotografii. În general, cu o singură armare se pot realiza 25 de poze. Cu cât aparatul produce mai puțin zgomot, cu atât este mai mult întrebuintat, chiar pentru fotografierea din apropiere și în locuri liniștite. Acesta este mascat în diferite obiecte, în special serviete sau poșete, de unde execută fotografierea. Înaintea expunerii se înlătură, manual sau mecanic, dispozitivul care maschează obiectivul foto și care este făcut din același material din care este fabricată servietea. Declanșarea se face de la un buton accesibil operatorului prin servietă, plasat în funcție de modul cum este purtată aceasta, iar mișcarea este transmisă mecanic la declanșatorul aparatului, cu ajutorul unor

pârghii. Reglajul aparatului, distanța, diafragma, timpul de expunere se prestabliste, cunoscând condițiile concrete de luminozitate și distanța la care se va executa fotografierea, iar încadrarea subiectului depinde numai de experiența operatorului și, spre mai multă siguranță, se 'trag' mai multe imagini.

Acesta este procedeul și aparatura care, de regulă, se folosește pentru fotografiari în exteriorul și chiar în interiorul unor localuri publice, când lumina este suficientă, după ce s-au luat în prealabil măsuri pentru a utiliza cele mai sensibile filme. Când este necesar să se lucreze în condiții de luminozitate redusă sau în întuneric, trebuie ca aparatura foto din servietă să fie completată cu o sursă de alimentare (acumulator) și o lampă asemănătoare blitzului folosit și în alte activități foto obișnuite. În fața lămpii se montează mascat un filtru infraroșu, reușind să se reducă astfel la minim lumina vizibilă emisă, lăsând să treacă spre subiectul vizat energia luminoasă în domeniul infraroșu sau o porțiune din aceasta, corespunzătoare cu sensibilitatea maximă a filmului infraroșu. Astfel, se pot executa, în secret, fotografii în exterior, în timpul nopții sau în încăperi cu luminozitate redusă. Dacă se cunoaște locul unde urmează să se desfășoare acțiunile ce trebuie fotografiate și acestea merită efortul material și uman, dispozitivele de produs lumină în infraroșu pot fi destul de puternice ca iluminare, iar obiectivele, teleobiectivele și transfocatoarele destul de sofisticate. Atunci, acestea trebuie ascunse în autoturisme, auto-dube etc. Probleme deosebite și multiple pune și fotografierea unor momente ce se petrec în interiorul unor camere, în special de hoteluri, moteluri, apartamente, care și ele, în prealabil, trebuie tratate special. Astfel, în diferite obiecte, ce se află în aceste încăperi ca: aparate de radio, televizoare, cărți din bibliotecă, unele piese de mobilier etc., se pot plasa aparate foto silențioase, de cele mai multe ori prin construcție destinate acestui scop care, fie că declanșează fiecare fotografie comandată de la distanță, printr-un sistem de emisie - recepție (pornire de la distanță), fie că, odată pornite tot de la distanță, ele fac automat sute de fotografii la intervale fixe, reglabile de la 5 la 20 secunde.

Astfel, într-o jumătate de oră, cât durează, în medie, o întâlnire secretă, se iau 90-360 imagini. Se deduce, din prezentarea acestor date, de ce este nevoie de un aparat foto de construcție specială. Acesta este în fond, un hibrid între un aparat

foto și unul de filmare cu care se obține o imagine mai mică decât cea standard. În el, trebuie introdusă peliculă de lungime mai mare decât cea existentă în casetele obișnuite (rolfilmele) cu număr clasic de expuneri. O caracteristică deosebit de importantă este, după cum am mai afirmat, silențiozitatea care se obține și din construcție dar și din blindarea aparatului cu materiale antifonice.

Dacă încăperile alăturate celei în care se află subiecții ce trebuie supravegheați și fotografiați, îndeosebi cele laterale, situații care se întâlnesc în hoteluri, apartamente în blocuri, pot fi puse la dispoziția (pe timpul acțiunii) celor ce fac observațiile și fotografiile, folosind aceeași aparatură, poate mai sofisticată, mai puțin silențioasă, dar, dat fiind spațiul mai mare avut la dispoziție pentru manevrarea și montarea aparatului, față de prima situație descrisă, se pot obține rezultate mai performante și, în mod sigur, există mai multă siguranță în asigurarea secretului acțiunii.

Singura problemă care se pune este modul cum se rezolvă contactul optic direct, dintre obiectivul aparatului de fotografiat, cu spațiul încăperii unde se află subiecții. Fără a intra în detalii, se pot evidenția mai multe procedee. Cel mai vechi este reprezentat de folosirea unei oglinzi speciale, care permite vizualizarea numai din camera unde se află spatele oglinzii și în care se montează aparatura foto, înspre cea unde se află subiecții ce urmează să fie supravegheați și fotografiați.

Cititorii rețin că, în multe filme polițiste acesta este procedeul când se dorește ca, în secret, un martor sau victima, să recunoască făptașul, dintr-un grup de persoane. Este de la sine înțeles că, în camera de observare sau în care este montată aparatura foto, trebuie să fie întuneric, spre deosebire de cealaltă, unde este nevoie de o lumină cât mai bună. O altă metodă este folosirea oricăror orificii care, în mod normal se află în cameră, ca cele din doze și prize electrice.

Se subînțelege că pentru a ajunge la acestea din încăperi trebuie să se înlăture porțiunea de zid pentru a putea plasa obiectivul aparatului foto cât mai aproape de doza sau priza din camera vecină. Cel mai modern și tehnic procedeu este folosirea unei sonde optice, de diametru în jur de 20 mm și lungime de aproximativ 250 mm, compusă dintr-un număr de lentile și prisme optice. Acestei sonde, care străbate zidul despărțitor, până la tencuiala camerei vecine, i se atașează la un capăt, printr-o montură specială, obiectivul aparatului foto, iar la cel opus, se

prevede un orificiu de 1-2 mm în tencuiala zidului care nu poate fi observat, decât la o cercetare atentă și astfel se pot efectua fotografii într-un câmp vizual de cca.65° în interiorul camerei supravegheate. Pentru a se înțelege mai bine, trebuie să ne imaginăm că acest obiectiv este o perfecționare a vizorului de la ușa unui apartament, prin care, cel din interior, poate vedea persoana din exterior, chiar dacă ea este plasată puțin lateral.

Deoarece, în acest capitol, ne-am referit la comanda de la distanță a pornirii sau opririi aparatului foto, vom prezenta numai informativ câteva date despre aparatura necesară acestei operațiuni. Emițătorul de comandă este de formatul unui aparat portabil de emisie - recepție, are o putere în jur de 5 W, lucrează în impulsuri și pentru siguranța operațiunii, posedă mai multe coduri lucrând în unde metrice. Receptorul care primește semnalul de comandă are o sensibilitate de 3 - 7 μV , cu un consum foarte redus în așteptarea semnalului; este de dimensiunea unei jumătăți de cutii de chibrituri și se montează lângă aparatul foto.

Aceleași aparate se folosesc și pentru pornirea și oprirea microemițătoarelor de interceptare dar din păcate și pentru treburi mai puțin ortodoxe, de către organizații teroriste, pentru detonarea de la distanță a încărcăturilor explozive.

Optoelectronica și televiziunea în serviciul contraspionajului

În continuare, vom prezenta unele din principalele mijloace electrono-optice de realizare a supravegheții fizice, în special în condiții de luminozitate scăzută și de urmărire a unor vehicule și persoane.

Până în 1969, singurele sisteme de vedere nocturnă erau cele bazate pe iluminarea în infraroșu, foarte asemănătoare cu cele pe care le-am descris la fotografierea în medii întunecoase. După această dată, a început era amplificatoarelor de lumină, la început cele de generația I.

Acestea s-au dezvoltat și perfecționat continuu, datorită cercetărilor din domeniul mijloacelor de luptă militare și s-a constatat eficiența acestora în războiul din Malvine, după cum am mai spus la începutul lucrării, dar și mai recent, în războiul din Golf

împotriva Irakului.

Dispozitivele respective funcționează la nivele scăzute de lumină cea de la lună, stele, ori de la lumina de fond, difuză a străzii, în timpul nopții. Imaginea este recepționată de videocaptatori și prin amplificarea luminii se obține o imagine acceptabilă pe micul ecran, permițând astfel vizualizarea.

După nici doi ani s-au pus la dispoziție intensificatoare de lumină (generația a II-a), de o mai bună calitate, asemănătoare cu cele ale televiziunii standard. Un intensificator pasiv de lumină are o lungime de 25-30 cm și este prevăzut cu un vizor de observare directă, totul este montat pe un mâner, la fel ca la video-cameră, pentru o mai ușoară și comodă manevrabilitate. Prețul unui astfel de echipament, cu obiectivele și transfocatoarele necesare, este de cca. 6000 dolari S.U.A. La iluminarea dată de o stea, după ce aparatul a amplificat lumina de circa 60000 ori, se poate repera o țintă umană de la 175 m.

Cu dispozitive mai mari, având o greutate de 20 kg și dimensiune de 75 cm, care se montează pe trepiede, în aceleași condiții de iluminare, un om poate fi reperat de la 1 - 1,8 km.

Nu trebuie să insistăm mai mult asupra faptului că pentru aceste sisteme de observare s-au creat dispozitive anexe ca magnetofone video și audio pentru că acestea au o largă răspândire și au devenit obiecte de casă. Trebuie însă arătat că s-au realizat emițătoare de mică putere, pentru transmis imaginea la punctele de observare pe care le vom trata când vom prezenta camerele de luat vederi.

Mai puțin scumpe sunt dispozitivele pasive de vizualizare nocturnă în infraroșu și care de obicei sunt prezentate în versiune binoculară, putându-se ține în mână, având sub 1 kg greutate. Ele detectează energia radiației infraroșii, reflectată sau emisă de subiect și o focalizează pe un tub electronic, care transformă infraroșul în lumină vizibilă. Un om se recunoaște de la 50 m, iar ca țintă de la 150 m și aceasta, datorită capacității lor de a detecta cantități foarte mici de energie calorică emise de corpul uman. Aceste dispozitive mai prezintă avantajul că atunci când condițiile permit se poate suplimenta energia în infraroșu, emițând-o nu numai la punctul de observare și îndreptând-o spre zona supravegheată. Sigur, în aceste condiții nu mai este vorba de sisteme de videocaptare pasive, dar faptul are mai puțină importanță dacă se obțin imagini mai performante.

Deși se folosesc camerele de televiziune clasice cu tuburi vidicon pentru observare și supraveghere, în sistemele de pază și alarmare, în prezent se analizează numai camerele construite cu video-captatori, pentru că sunt făcute pentru situații deosebite. Acestea, deși au o calitate mai slabă ca cele din televiziunea clasică (dar care nu deranjează pentru scopul pentru care au fost create), dimensiunile foarte mici și posibilitatea de a prelucra semnalul video le fac foarte interesante și răspândite pentru cazuri speciale. Videocaptatorul cu semiconductori este construit dintr-o matrice cu peste 10000 de senzori de lumină, microminiaturizați și care poate fi asamblată pe o suprafață de 6,3 x 6,3 mm, sau cu dispozitive captoare de imagini bidimensionale de tip CCD.

Dacă aceasta se completează cu obiectivele necesare și circuitele electronice adecvate, se realizează o cameră completă de televiziune miniaturizată, de dimensiunea 100 x 50 x 45 mm, cu o greutate de 300 g, care poate lucra între 0,2 - 1000 lucși.

Aceste camere pot fi cuplate cu fibre optice speciale (pentru imagini și nu numai pentru lumină) și se realizează visul de a capta imaginii 'colțite' sau 'după colț' (foarte interesante pentru fotografiile și observările dintr-o cameră în alta.

Aceste aparate, dacă nu este necesar să se transmită imagini video în alte locuri, se cuplează la receptoarele de televiziune cu circuit închis, de tipuri comerciale clasice, dar care, în prealabil, au fost adaptate, după caz, și la video-magnetofone.

Dacă se dorește ca imaginea captată să fie transmisă, clar sau cifrat, la o anumită distanță, de ordinul câtorva kilometri, de exemplu, se cuplează la un emițător TV. Cei mai răspândiți radioemițători TV funcționează în gama 400 - 900 MHz, au o putere de 2-5 W, cântăresc până la 1,5 kg și au dimensiunea de 50 x 50 x 100mm, fără sursa de alimentare.

Altele, mai moderne, de dimensiuni și mai mici, în greutate de 300 g, în gama undelor centimetrice, de putere până la 20 mW, cu antena încorporată, au rezultate foarte bune, cu protecție la perturbații și interferențe.

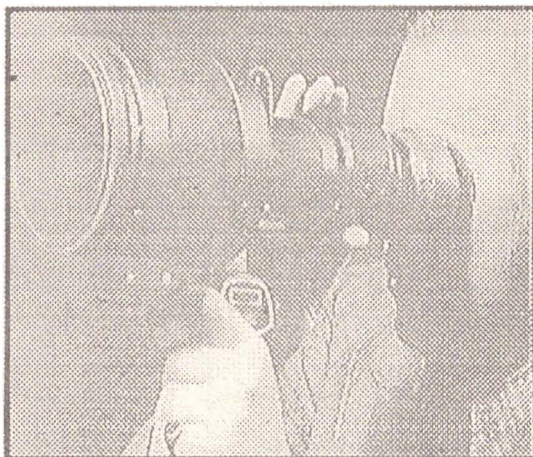
Principalul avantaj al camerelor cu semiconductori, pe lângă cele asupra cărora am insistat, derivă din posibilitatea de prelucrare cu procedee speciale a imaginii, pentru îmbunătățirea acesteia (a contrastului, a intensității și varierea treptelor de gri) ceea ce ar fi imposibil prin sisteme clasice. Se pretează și la prelucrarea în vederea cifrării imaginii, pentru a se asigura un

anumit grad de secretizare a transmisiei. Este o codare care duce la o imagine neinteligibilă și nu așa cum sunt obișnuiți unii dintre cititorii noștri care au urmărit emisiuni TV prin satelit și în care există așa-zise transmisii codate, dar în care se înțelege despre ce este vorba în imagine, fiind mai mult o incitare la cumpărarea decodorului.

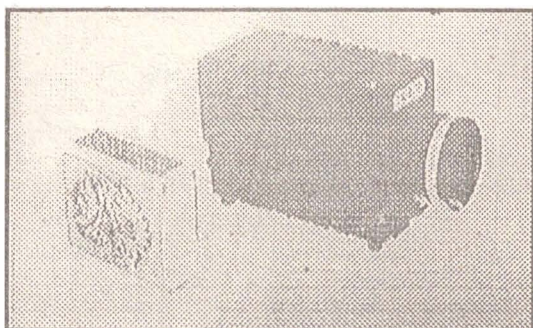
Localizarea emițătoarelor pentru depistarea persoanelor

Pentru cei care nu sunt familiarizați cu principiul de funcționare al radiogoniometrului, amintesc că este vorba de un receptor cu o antenă rotativă specială, pentru stabilirea direcției câmpului maxim, care este în același timp și direcția în care se află emițătorul baliză. Dacă sunt trei astfel de goniometre și trasăm direcțiile pe un plan (hartă), vom obține un triunghi (la limită poate fi un punct), în interiorul căruia se află emițătorul baliză. Se înțelege că, dacă emițătorul este plasat la o persoană sau mașină urmărită, ne atingem obiectivul propus de a ști unde se află la un moment dat acesta. Teoretic, totul este deosebit de ușor, dar în practică este greu de plasat emițătorul baliză fără ca persoanele supravegheate să nu observe acest lucru. Emițătorii baliză au puteri de la 50 mW până la 1 W și cu baterii proprii, au dimensiuni de 75 x 50 x 125 mm obținând o bătaie, în oraș, de 10 - 100 m, iar în câmp deschis, de 2 - 5 km. Receptorul goniometru modern folosește, pentru stabilirea direcției emițătorului baliză, în loc de antena cadru, cum s-a văzut în filmul "Sorge" și care era folosit în cel de-al II-lea război mondial, tehnici de măsurare de tip interferometric.

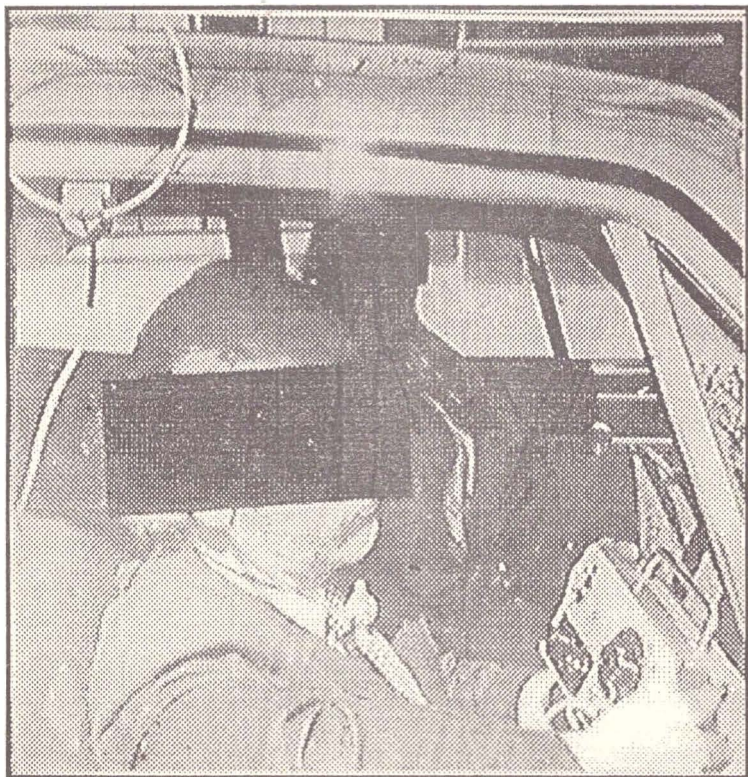
Operatorului care, să presupunem, se află cu goniometrul într-un mijloc auto, urmărind o altă mașină în care se găsește emițătorul baliză, faptul că acesta se află în raza de acțiune a goniometrului îi este semnalat nu numai prin indicatori acustici, ci și cu ajutorul unui instrument cu ac, cu posibilitatea deplasării dreapta-stânga, care arată direcția spre obiectiv și îi indică mișcarea relativă.



- Dispozitiv de observare pe timp de noapte, cu ajutorul razelor infrarosii



Camera de luat vederi miniaturizata



Receptor gonlometric pentru urmarirea si localizarea
autoturismelor ce au montate emitatoare baliza

S-au construit emițători baliză de puteri și mai mari care se alimenteze de la acumulatorul mașinii, de 1-3 W, având o bătaie sol - sol de până la 7 km. Sunt prevăzuți cu posibilitatea decuplării manuale, dar și prin telecomandă, de la baterla mașinii.

Pentru a da indicații nu numai asupra direcției ci și asupra distanței, baliza emite cu putere mare într-un anumit ton peste 1000 Hz, iar cu putere mică, o modulație sub 1000 Hz. Dacă operatorul le aude pe amândouă, înseamnă că radio-baliza este aproape iar, dacă îl aude numai pe primul, este departe. Așa cum a fost descris emițătorul care trebuie să fie urmărit este bine știut că este vorba de celebrul "beep-beep" care prin anii '75 a făcut vogă în presă, făcându-i-se o zgomotoasă reclamă.

Adevărul este că în mediul urban se întâlnesc, în aplicarea acestui sistem, greutăți deosebite, datorită reflexiilor multiple din cauza clădirilor, precum și a modificărilor permanente ale traseelor de propagare dintre cele două vehicule. Acest sistem tehnic se folosea prin anii '60 - '70 în țările din America de Sud, cu avizul și cunoștința persoanelor urmărite, de fapt proprietarii mașinilor, pentru descoperirea personalităților politice importante care erau răpite împreună cu autoturismele lor, de către organizații adverse. Pentru acest scop, în autoturismele persoanelor care constituiau ținte probabile pentru aceste organizații, se montau în condiții lejere, radiobalizele, având grijă ca emisiunea să aibă un cod propriu de recunoaștere iar antena să fie montată în condiții cât mai degajate. Găsirea ulterioară a mașinii folosind goniometrul putea oferi date și informații relevante asupra locului unde se afla persoana răpită. Sunt folosite, în special pentru unele situații, și alte principii de goniometrie bazate pe diferența de timp de propagare, sistemul de localizare pe bază de coordonate în diferite variante dar, având în vedere tematica lucrării, nu vom insista asupra acestora.

Vom arăta însă că principii asemănătoare, dar cu unele diferențe și în alte scopuri, sunt folosite de către poliția unor metropole. Astfel, mașinile acestora sunt dotate cu emițători de mică putere, fiecare cu indicatorul său de cod. Pe străzile orașului sunt plasate receptoare la o distanță convenabilă care, la rândul lor, sunt legate la un panou central la dispeceratul poliției. Când o mașină intră în zona de 'prindere' a unui receptor, indicativul acesteia este transmis pe panoul luminos la care m-am referit. Astfel, în orice moment se poate urmări cum sunt dispersate

mașinile poliției pe străzile orașului și acest lucru prezintă avantaje deosebite în situații speciale (spargerii, crime, vizite importante etc.).

Depistarea emițătoarelor folosite în activități de spionaj-tradare

Problema depistării emițătoarelor baliză pentru supravegherea persoanelor s-a tratat, iar într-un viitor capitol vom aborda și problema găsirii celor care sunt folosite pentru interceptarea convorbrilor. Până în prezent s-au prezentat puține date despre ascultarea și localizarea emițătoarelor întrebuințate în transmiterea informațiilor la mare distanță în scopuri de spionaj-trădare (Capitolul al XI-lea).

Fiecare stat cu o anumită dezvoltare economico-socială are organizată activitatea de interceptare a emisiunilor radio și apoi de localizare a celor neautorizate, clandestine. Rezolvarea acestei sarcini începe prin aprobarea funcționării, prin asigurarea unei evidențe foarte precise a tuturor emițătoarelor și frecvențelor de lucru, indicativelor, precum și a amplasamentelor folosite de acestea. Pentru a se înțelege mai bine se poate spune că aceasta este o activitate asemănătoare cu cea desfășurată de Consiliul Audiovizualului (C.N.A.) din țara noastră, dar nu numai pentru stațiile de radio și televiziune ci pentru toate emițătoarele ce funcționează în țară, deci și ale poliției, armatei, aviației, taximetrelor, stațiilor de salvare, guvernamentale și altele. Este absolut necesar ca evidența acestora să fie la dispoziția serviciului de contrainformații radio, indiferent cărei instituții centrale aparține acesta: Ministerul Telecomunicațiilor, Ministerul Apărării Naționale, Ministerul de Interne, Servicii de Informații sau Contrainformații. Ceea ce contează nu este apartenența acestor organisme, ci dotarea lor cu aparatură modernă și încadrarea cu personalul necesar. Să ne imaginăm că nu există această evidență. Centrul de ascultare depistează o emisiune radio și apoi desfășoară toate forțele tehnice și umane pentru localizarea emițătorului, ca să constate în final că provine de la o stație de emisie oficială, autorizată, poate militară, poate a unei instituții de telecomunicații, a unui radioamator etc. Se poate imagina ușor că

emisiunile sunt infinit mai numeroase decât cele de spionaj, așa că, în cazul inexistenței evidenței nu se poate imagina obținerea de rezultate în localizarea celor clandestine pentru că se efectuează inutil multă muncă. Activitatea devine eficientă dacă, după interceptarea emisiunii se consultă evidența stațiilor de emisie autorizate, pentru a fi eliminate cele cunoscute iar acțiunea de goniometrare se va putea concentra numai doar pe cele suspecte de spionaj-trădare. Deși toate acestea par de la sine înțelese s-au prezentat totuși, pentru a arăta cât de periculoase și fără sens au fost discuțiile care s-au purtat după Revoluția din decembrie 1989, privind existența evidenței stațiilor de emisie militare la Centrul de Contrainformații radio însărcinat cu depistarea emisiunilor neautorizate.

Toate țările își autorizează și organizează evidența posturilor de emisie, respectând convențiile și reglementările internaționale (anexa I-a). Fără ordine, reguli și evidență riguroasă nu pot exista comunicații radio. Toate țările au centre de ascultare (interceptare), bineînțeles cu mari diferențe între ele, determinate de puterea economică a statului și interesul manifestat de acesta. Diferențele se fac simțite în existența a mai multe sau a mai puține centre de interceptare și în cadrul lor în: numărul de posturi de supraveghere radio, calitatea receptoarelor (manuale sau automate), benzile radio supravegheate, colaborările pe care le au cu alte centre similare pentru a contracara efectele condițiilor de propagare.

În unele țări occidentale ca în Anglia, la centrul de ascultare din Caversham Park (65 km de Londra, nu departe de Oxford) se monitorizează, pentru nevoile B.B.C., tot ce se emite și se poate asculta în benzile de radiodifuziune, dar centrul satisface și toate necesitățile Ministerului de Externe, Ministerului Apărării, ale Serviciilor de Informații și Contrainformații fără a căror "sponsorizare" centrul B.B.C. de la Caversham ar da faliment. Cel de la Fort-Meade (Maryland - S.U.A.) inaugurat în 1957 de N.S.A. (Agenția de Securitate Națională) este dotat cu cele mai moderne mijloace de interceptare, decriptare și de stocare a informațiilor cu ajutorul ordinarilor, fiind încadrat cu un personal de peste 20000 de specialiști. Acesta își propune în primul rând să asculte rețelele radio (cifrate sau clare) guvernamentale (legăturile statelor cu ambasadele lor), militare, ale tuturor țărilor care prezintă interes pentru S.U.A. Concomitent

se acţionează şi pentru depistarea staţiilor clandestine din interiorul ţării.

Germania, prin construirea noului şi ultramodernului centru "Castagnete" din Schlesing Holstein îşi propune să facă din acesta o "ureche" căreia să nu-i scape nimic din ceea ce se emite în eter, atât din ţară cât şi din cele mai îndepărtate zone de pe mapamond.

În fostele ţări socialiste participante la Tratatul de la Varşovia, centrele de ascultare şi de goniometrie erau specializate numai pentru depistarea staţiilor suspecte de activităţi de spionaj-trădare şi erau strict coordonate prin stabilirea amplasării acestora pe teritoriul fiecărei ţări, determinarea numărului de posturi de interceptare şi a criteriilor de prioritate în activitatea de supraveghere şi goniometrie, stabilirea benzilor de frecvenţă baleiate pentru fiecare centru, asigurarea dotării respective.

Acest sistem de organizare era justificat de condiţiile de propagare radio care fac ca o staţie de emisie de putere de 30-100 W în unde scurte, ce emite pentru un centru de spionaj aflat la 2000 - 3000 km să poată fi interceptat pe o rază de 10 - 20 km, după care pentru sute de km există o zonă de "tăcere".

Deoarece în organizarea la care s-au făcut referiri a fost mai multă coordonare sovietică decât cooperare, pentru a înlătura efectele negative ale zonelor de tăcere, România (singura ţară) în prima jumătate a anilor '60 s-a retras din acest aşa-zis mic Tratat de la Varşovia pentru contrainformaţii radio şi apoi şi-a dezvoltat propriul său sistem de supraveghere şi localizare radio. Depistarea unor emisiuni radio clandestine în eter este un succes, dar până la localizarea emiţătorului mai este de parcurs încă o cale lungă. Comanda manuală sau automată, cu transmiterea tuturor datelor de identificare a emisiei (în special frecvenţa acesteia), trebuie făcută foarte rapid la cel puţin trei centre fixe de goniometrie, care trebuie să "prindă" şi ele emisiunea respectivă şi să obţină direcţia (azimutul) staţiei emiţătoare, pe baza audiţiei maxime. Cele trei direcţii puse pe o hartă dau, de regulă, un triunghi ce reprezintă, în teren, o suprafaţă de circa 30 km². Zona respectivă va fi încadrată ulterior cu 3-4 goniometre plasate pe mijloace mobile şi se aşteaptă o nouă apariţie în eter. În cazul fericit că aceasta va avea loc în aceeaşi zonă, se repetă operaţia, de data aceasta cu goniometre mobile şi se poate obţine localizarea

emiiătorului, dar de cele mai multe ori numai reducerea suprafeiei zonei. La o nouă emisiune va trebui să se intervină cu goniometre portabile pe corpul lucrătorilor de contrainformații radio. Toată această activitate se desfășoară contra cronometru și rezultatele operative sunt greu de obținut când emisiunile, astăzi, durează câteva secunde. Dar despre perfecționările necesare în acest domeniu se vor mai face referiri.

Pentru a sublinia cât de importantă este folosirea mijloacelor tehnice în urmărirea și depistarea unor emiiătoare și a altor dispozitive vom reda în continuare modul cum este tratată această problemă într-un săptămânal de mare tiraj. Astfel, în săptămânalul american "Newsweek" din 18 octombrie 1993, a fost inserat articolul "*Când personajul negativ nu are telefon care să poată fi interceptat*", semnat de Douglas Waller, corespondentul revistei la Washington. Redăm traducerea integrală:

"De ce nu poate fi prins Mohamed Farah Aidid ? Trucurile obișnuite ale autorităților de la Washington nu funcționează în acest caz. Cadrele C.I.A. își îndeplinesc, de regulă, misiunile de spionaj în țările lumii a treia mituind oficialitățile guvernamentale în schimbul informațiilor. Agenția Națională de Securitate culege informații folosind interceptarea convorbirilor telefonice. Dar în SOMALIA nu există oficialități guvernamentale și prea puține telefoane. Aidid vorbește doar foarte rar la radio, preferând mesagerii. Pentagonul încearcă să folosească echipament radar pentru a localiza centrele de unde își transmite generalul mesajele. Dar Aidid folosește un transmițător mobil cu arie mică de difuzare care funcționează sfidând toate regulile tehnicii și făcând imposibilă detectarea lui. 'Tehnica arhaică înfrânge tehnologia avansată', spune un consilier de la Pentagon."

"Capacitatea de pătrundere a Washingtonului a fost 'aproape total nefolositoare în Somalia', spune președintele Comisiei pentru probleme de informații a Camerei Reprezentanților, Dan Glickman. Baza de operații a lui Aidid din sudul capitalei Mogadiscio a devenit o enclavă pe care agenții de penetrare ai C.I.A. (mulți dintre aceștia fiind racolați din rândul membrilor clanurilor rivale) nu îndrăznesc să o abordeze. 'Este un climat ca la Beirut', spune o oficialitate americană din cadrul comunității informative."

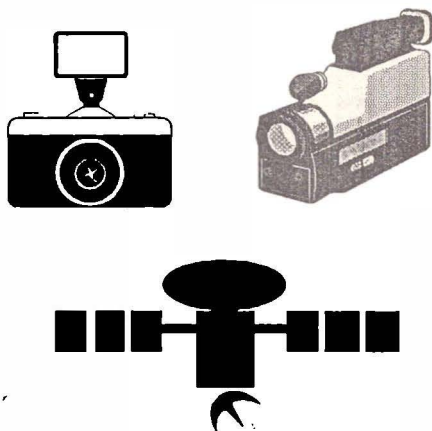
"Agenții din clanurile ostile sunt identificați cu ușurință,

iar cadrele C.I.A. se confruntă cu aceleași pericole ca și ceilalți soldați aflați în teren. Reporterul revistei 'Newsweek' a aflat că un cadru C.I.A. a fost rănit luna trecută într-o ambuscadă. Este a doua victimă în Somalia din rândurile C.I.A."

"Națiunile care au trimis forțe de menținere a păcii sub egida O.N.U. nu sunt de ajutor; se bazează pe propriile lor servicii de spionaj și nu împart cu partenerii din coalțiie informațiile obținute. 'Natiunile Unite sunt atât de neîncrezătoare și temătoare de operațiunile de culegere de informații încât au și șters această sintagmă din vocabularul lor', spune Jack Reed, membru al Comisiei pentru probleme de informații a Camerei Reprezentanților".

"Trupele de comando 'Delta' se află în Somalia cu sarcina de a-i salva pe soldații americani ținuți ostateci după raidul din 3 octombrie. Dar forțele 'Delta' au nevoie de cel puțin trei ore ca să pregătească o operațiune de salvare și de un agent infiltrat ca să le indice locul unde sunt deținuți ostatecii. 'Găsirea ostatecilor va fi tot atât de ușor de realizat ca și găsirea lui Aidid', recunoaște un ofițer american. Pentru a-i descoperi și salva, cea mai sofisticată operațiune de spionaj din lume va avea nevoie de ceva ce i-a lipsit până acum - o ocazie norocoasă".

Trupele americane vor fi retrase din Somalia, poate și din aceste motive.



CAPITOLUL XIII

METODE ȘI APARATURĂ PENTRU DEPISTAREA INTERCEPTĂRIILOR TELEFONICE, A ALTOR SISTEME DE ASCULTARE CU FIR ȘI DE PROTECȚIE ÎMPOTRIVA ACESTORA

Este bine cunoscut faptul că orice armă sau metodă nouă creează o contraarmă și noi posibilități de apărare care, la rândul lor, duc la inventarea unor noi mijloace ofensive. Folosirea sabiei și a arcului cu săgeți a dus la apariția armurii și protecției luptătorilor cu zale care apoi s-au dovedit ineficace în fața armei de foc cu glonț. Cetățile, ca mijloc de apărare, au dus la inventarea și folosirea în luptă a scării și berbecului de asalt și mai apoi a tunului. Eficiența acestuia din urmă a fost descrisă de V. Corbu în "Căderea Constantinopolului" și a dus la ocuparea lui de către trupele otomane.

Radioemițătoarele, în prima parte a celui de-al doilea război mondial, ca mijloc de transmitere a informațiilor obținute din activitatea de spionaj, au fost invulnerabile dar, după apariția și perfecționarea goniometrelor acestea au început să fie descoperite și localizate unul după altul.

Cei care au văzut filmul "Sorge" își reamintesc cum, echipe de contraspionaj japoneze, dotate cu goniometre germane, localizau radiotransmisiile făcute de telegrafistul rețelei de spionaj condusă de cel care a dat și titlul filmului.

În prezent, când emițătoarele transmit cu viteze foarte mari (o pagină de informații în câteva secunde) și cu multiple frecvențe care se schimbă după un anumit program, goniometrele, necunoscând încă noi perfecționări, au devenit ineficiente. Se mai pot da multe alte exemple, dar importante de reținut sunt concluziile care se impun. În primul rând, mijloacele de apărare sunt mult mai greu de realizat și mai costisitoare. Nu este ușor să fabrici și să arunci o bombă atomică, dar infinit mai greu este să te aperi de aceasta. Costă enorm fabricarea și punerea pe

traiectorie a unei rachete intercontinentale, dar metodele de apărare împotriva acesteia, prevăzute în programul "Războiul stelelor", sunt așa de costisitoare, încât un stat ca fostul U.R.S.S. nu și-a putut permite cursa, a renunțat la războiul rece și la ideologia care-l guverna. În al doilea rând, în lupta dintre mijloacele ofensive și cele defensive nu există permanent un echilibru stabil și la un moment dat unele dintre acestea, de obicei cele ofensive, o iau mult înaintea celorlalte, dar sunt și multe cazuri, pentru perioade scurte, când se întâmplă și situații inverse. Nici mijloacele de interceptare, de transmitere, de cifrare nu se puteau sustrage acestor reguli și apariția lor a dat naștere unor metode, procedee și tipuri noi de aparatură, a unei întregi industrii înfloritoare, pentru depistarea, localizarea, contracararea sau protecția împotriva acestora.

•

• •

Literatura de specialitate este plină de termeni ca audio - countermeasures (A.C.M.), technical security countermeasures (T.S.C.M.), debugging (deparazitare), audio surveillance (supraveghere audio), device detection (dispozitive de detectare) sau penetration prevention, pe care nu mai trebuie să-l traducem.

Așa cum am procedat la prezentarea metodelor de interceptare, la fel le vom descrie separat și pe cele de contracarare a ascultărilor, cu ajutorul telefoanelor, a microamplificatoarelor și a emițătoarelor (în general a tuturor celor numite interceptări fără fir). Nu vom lăsa la o parte nici procedeele și aparatura necesară contracarării radioemițătoarelor și a mijloacelor foto-chimice de transmitere a informațiilor și a altor metode, la care ne-am referit în capitolele anterioare.

**Interceptarea convorbirilor telefonice
nu este infailibilă. Cum ne protejăm
și cum o depistăm ?**

Înainte de a prezenta depistarea sau protejarea împotriva interceptării convorbirilor telefonice, trebuie să arătăm că cele mai

eficiente și sigure metode de protecție sunt evitarea transmiterii unor informații secrete prin telefon sau folosirea unor secretizoare audio de bună calitate. Dacă prima metodă nu necesită explicații suplimentare, cea de-a doua merită o tratare specială, pentru că s-a dezvoltat mai ales în ultimul timp. Tehnica secretizării, a "scramblers", cum este cunoscută în literatura de specialitate, a dus la construirea unor aparate foarte diverse, de la cele mai simple, care costă 400 dolari S.U.A. perechea, la câteva zeci de mii, cele mai perfecționate. Teoria care stă la baza proiectării și realizării scramblerelor a fost descrisă în multe lucrări, dar o prezentare succintă, rezumativă, a tuturor principiilor folosite, după consultarea unei vaste bibliografii, este cea realizată de Arnold M. Mc. Colmant de la Tehnical Communications Corp Lexington Massachusetts, pe care o recomandăm și care arată că până în 1975, erau circa 25 patente în domeniul secretizării vocii. Cele mai simple, dar foarte eficiente pentru "o simplă ureche indiscretă" folosesc inversiunea de frecvențe. Banda vocală este prelucrată în domeniul frecvență și, prin procedeul clasic ce folosește un modulator echilibrat, comandat de un oscilator cu frecvență fixă și cu filtre pentru suprimarea benzii laterale superioare, se realizează inversiunea de frecvențe și, implicit, o anumită secretizare. Astfel, frecvențele joase, în jur de 300 Hz, se transformă în frecvențe înalte, în jur de 2700 Hz și invers (de aici și denumirea metodei). Pentru a crește gradul de secretizare s-au imaginat oscilatoare cu mai multe frecvențe, comandate la dorința utilizatorului prin comutatori sau frecvențe variabile, alese după un anumit algoritm. Altele, și mai costisitoare, împart banda de frecvențe în 5 sau 6 subbenzi de 600 sau 500 Hz fiecare, pe care le transpun și le transmit într-o ordine stabilită. A fost perfecționată și aceasta, obținându-se metoda "Dynamic 'M' ary rolling cod" la care fiecare segment de transmisie are o ordine schimbată a subbenzilor. Pentru realizarea acestor metode se folosește atât prelucrarea în domeniul frecvență, cât și în domeniul timp a semnalului vocal. Din punct de vedere al modului de prezentare constructivă se menționează două tipuri principale. Primul este o construcție simplă, portabilă, care se cuplează acustic cu microreceptorul telefonic. Caracteristic acestui tip este aparatul Hand - Set - Scrambler CC - 400, cu peste 50000 de chei, fabricat în 1991 de Communication Central System (C.C.S.). Altele, mai sofisticate, sunt fixe și se cuplează electromecanic cu

aparatul telefonic. Un astfel de tip este cel realizat de firma Technical Communication Corporation tipul 207/307 care folosește metoda M.R.C., cu aproape 300000 chei.

Un foarte utilizat aparat de cifrare a comunicațiilor pe căi telefonice este cel pe care-l vom descrie în continuare. El este construit și montat într-o servietă diplomat, pentru a putea fi ușor transportabil. Mesajul ce urmează a fi transmis este înscris cu ajutorul claviaturii aparatului, asemănător executării acestei operații la mașina de scris electrică și este introdus într-o memorie electronică capabilă să înregistreze datele de pe 1-2 pagini format A₄. În drumul său spre canalul telefonic, mesajul clar este amestecat cu o cheie internă a aparatului de secretizare, obținându-se astfel semnalul cifrat în banda audio.

De la un post telefonic, operatorul obține în prealabil legătura cu corespondentul căruia dorește să-i transmită mesajul și, după discutarea problemelor banale și verificarea calității legăturii, pune microreceptorul telefonului într-un lăcaș special amenajat în aparatul de secretizare, deoarece cuplajul se face acustic, nefiind nevoie de a se umbla la legăturile aparatului telefonic sau la cablul acestuia. La apăsarea unui buton mesajul, în prealabil menșurat și cifrat, este introdus sonor în microreceptor și de aici prin legătura telefonică stabilită și verificată, cu o viteză de 34 caractere pe secundă ajunge la destinație. Aici, cu dispozitive similare, mesajul este decodificat și bătut la mașină sau redat pe un aparat telex.

Metoda este deosebit de utilă și folosită de delegațiile economice, când tratează afaceri în țări străine și trebuie să țină legătura cu instituția sau organizația pe care o reprezintă și când secretul trebuie păstrat câteva zile, până la încheierea afacerii. Confidențialitatea transmisiei nu poate fi asigurată pe termen lung, dacă cei interesați în decriptare folosesc ordinatoarele în activitatea de aflare a textului clar.

Aparatura de cifrare a comunicațiilor telefonice a luat în ultimul timp o mare dezvoltare așa cum rezulta și dintr-un supliment al cotidianului german "Frankfurter Allgemeine" din 4 august 1992 în articolul *"Cum rămâne secretă o convorbire telefonică; secretizarea devine o tehnică tot mai solicitată și de alții decât utilizatorii din armată și organele de stat"* de Gerd Gregor-Feth și din care reținem:

"Mult trâmbișatul sfârșit al așa-numitului război rece a

adus pentru industria comunicațiilor o cerere sporită de produse care necesită cunoștințe de criptologie și care până nu de mult erau destinate unor grupuri extrem de reduse de clienți. A crescut importanța transmisiilor radio mobile, a telecopiatoarelor și a transmiterii datelor la distanță. Persoane particulare dar și firme doresc să se apere de 'ochi și urechi' nedorite. Industria nu avea voie să livreze echipamente necesare oricui pentru că aparatura de codificare putea fi folosită doar de organele de stat sau cele militare. Vânzarea către persoane particulare era strict interzisă. Pe de altă parte, personalul tehnic specializat în interceptare se poate recruta astăzi mult mai ușor".

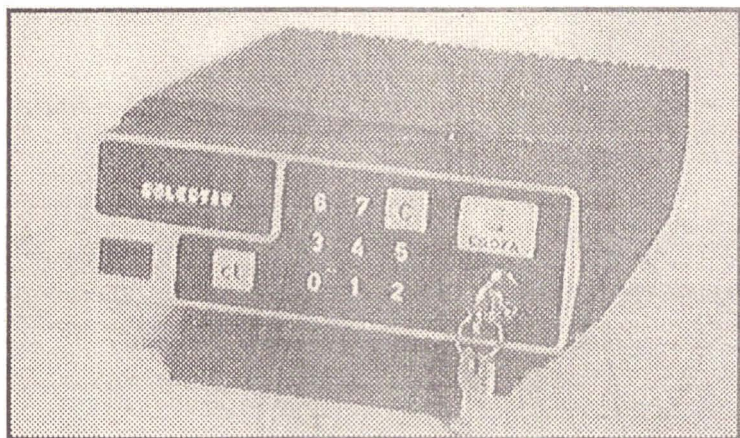
Firma "Siemens" a reușit să pună la punct în 1991 aparatul de secretizare telefonică în sistem analogic Crypset 100 utilizabil în toată lumea, care a primit pentru prima dată aprobarea Poștei germane ca secretizor de telefonie.

În prezent se produce modelul digital Crypset 300, care poate fi interconectat la rețeaua-ISDN (Rețeaua Digitală Integrată pentru Servicii) printr-un aparat telefonic suplimentar "Siemens Hi-Com". Instalația este comercializată de la sfârșitul anului 1992 și costă circa 10000 mărci, ca și Crypset 100.

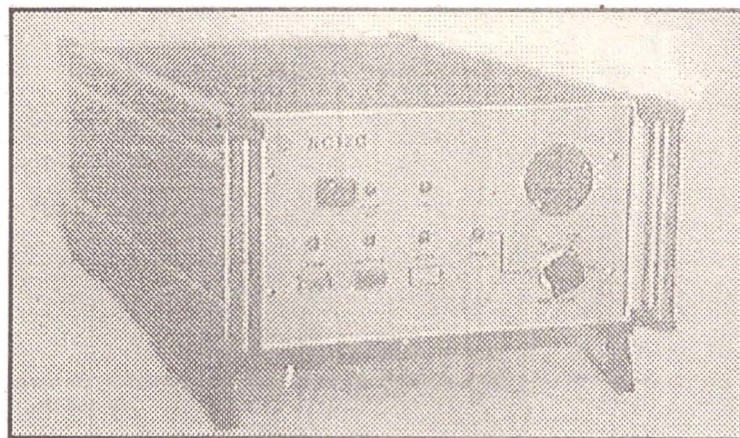
Concernul german nu este primul care lansează pe piață telefoane garantate împotriva interceptării. Firma americană "Motorola" vinde de cinci ani modelul Sectel SV X 2400, în S.U.A., care este permis și în majoritatea țărilor europene, iar pentru modelul SV X 9600, firma a primit aprobarea să-l vândă și în Germania.

În Franța firmele Sagem și Thomson, iar în Italia firma Telsi oferă de câțiva ani secretizoare telefonice. Chiar și firma germană Telecom simte cererea mare și de aceea la expoziția din 1991 a anunțat că o filială a sa oferă servicii în domeniul Telesec (secretizarea telecomunicațiilor) care vor fi oferite în cursul anilor viitori. Prețul aparatului I.S.D.N. Octophon și a lectorului de cartele este de circa 5000 mărci; secretizarea costă lunar 40-50 mărci.

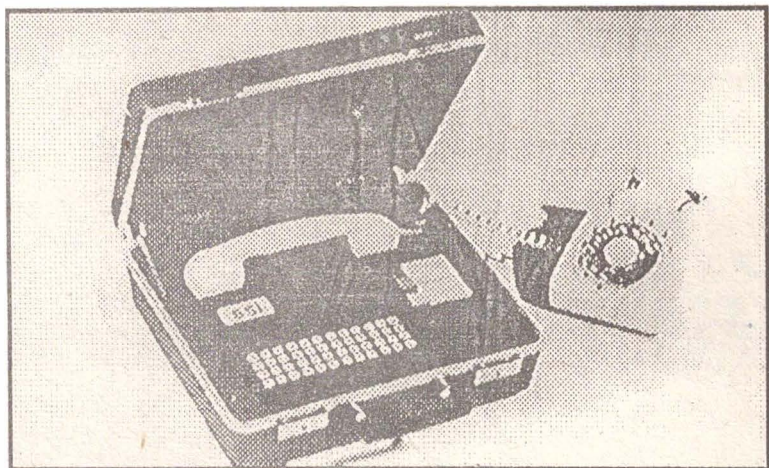
Se pot imagina, proiecta și realiza aparate de secretizare foarte complicate, cu o prelucrare atât în frecvență cât și în timp a semnalului vocal cu sisteme de codare pseudoaleatoare, dar caracteristicile slabe ale canalului de transmisie, în cazul de față cablul telefonic, mai ales banda îngustă de frecvență, așa numita bandă de trecere și greutatea de sincronizare a perechii de aparate



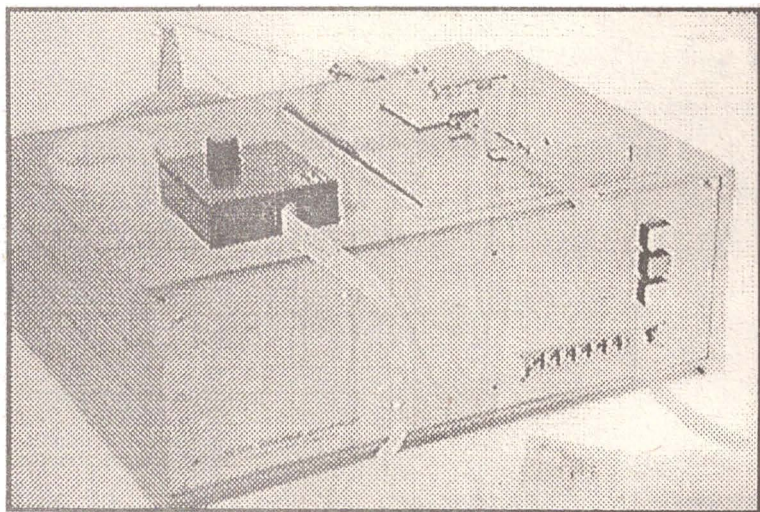
Aparat sofisticat pentru cifrarea mesajelor



Dispozitiv pentru cifrarea comunicatiilor telex care foloseste generator intern pseudo-aleator programabil.



Aparat pentru secretizarea comunicatiilor telefonice.



Dispozitiv pentru secretizarea transmisiilor telex cu banda perforata aleatoare.

de secretizare fac ca, în cele din urmă, acestea să nu poată fi întrebuințate decât pe canalul radio, pentru codificarea convorbirilor radio-telefonice, în special din mijloace mobile. Un astfel de aparat, cu scopul pe care l-am arătat, cu un număr de 65000 de chei și cu o perioadă de repetiție a generatorului pseudoaleator de 2×10^{20} , în cazul unei funcționări continue, s-a realizat, pentru întrebuințări speciale, de către un institut de cercetări din țară.

Panoul de comandă al acestui aparat, care n-are nici un caracter ofensiv, a fost prezentat, în zilele fierbinți ale Revoluției, la TV de un așa-zis inginer, ca declanșator cu încărcătură explozivă pe care, chipurile, prezentatorul ar fi dezamorsat-o. Ai voie să nu știi ce este un aparat sau o parte din acesta, dar n-ai dreptul să fabulezi și încă în momente deosebit de grave.



Să revenim, însă, la problemele depistării tehnicii de interceptare, pentru că, ceea ce s-a prezentat până aici nu detectează tehnică de interceptare ci o face inefficientă, o contracarează.

Se susține că nu există o singură metodă infailibilă, ci sunt mai multe teste și controale care trebuie realizate și ale căror rezultate și date obținute se coroborează între ele, pentru a avea rezultatul dorit, și anume localizarea și înlăturarea tehnicii de interceptare sau obținerea certitudinii că aceasta nu există. Astfel, dacă la un control fizic al aparatului telefonic, al cablului până unde acesta poate fi inspectat, adică până la prima sau următoarea cutie, din holul blocului, pe fațada casei sau stâlpului telefonic, descoperim o derivație clandestină, ne putem felicita, pentru că aceasta ne va duce, în cele din urmă, la dispozitivul de interceptare. Dacă n-o găsim, nu înseamnă că putem afirma că nu există derivație și deci interceptare, pentru că aceasta se poate face în foarte multe locuri, între centrală și aparatul telefonic.

În afara inspecției vizuale, s-au realizat aparate ai căror constructori pretind că exploatează capacitatea sistemului telefonic de a stabili existența unor modificări pentru interceptare și că vor fi detectate derivațiile ilegale. Afirmațiile sunt greu de crezut, deoarece caracteristicile liniei telefonice, parametrii ei

electrici, variază în funcție de starea vremii, umiditate, temperatură și lungimea ei până la centrală etc. Acestea produc variații mai mari decât cele datorate derivațiilor de interceptare cu dispozitive eficiente și de calitate.

Alte aparate de control folosesc sisteme mai complicate, recurgând la trimiterea pe linile telefonice controlate de impulsuri electrice. Acestea sunt reflectate de către joncțiunile electrice (eventuale derivații) înapoi la sursă. Față de o situație mai veche, cunoscută, o derivație apare la acest test ca o nouă joncțiune. Această metodă de detectare poate fi folosită doar în situații în care se cunoaște foarte bine tot istoricul instalării sistemului telefonic, al traseului său până la centrală.

În orice caz, controalele și verificările periodice pot evidenția situațiile noi care apar. Această tehnologie, denumită reflectometrie în domeniul timp, fiind complexă și rezultatele măsurătorilor necesitând interpretări, este bine să fie elaborată și executată de către cadre tehnice calificate, care practică aceste controale la multe linii telefonice și au o anumită experiență.

Trebuie să se rețină faptul că în aceste controale de mare utilitate sunt instrumentele universale electrice (așa numitele volt-ampermetre) care nici nu sunt scumpe și cu care se pot măsura tensiunea și curenții electrici.

Dacă pe întregul parcurs al cablului, de la centrală până la telefon, nu există dispozitive de interceptare care consumă curent din rețeaua telefonică, tensiunea de la centrală trebuie să fie, în linii mari, egală cu cea de la bornele aparatului telefonic. Dacă în rețeaua telefonică, la un post al acesteia, când receptorul este pe furcă, în loc de 48V se măsoară o tensiune mai mică cu 7 - 8 V, sau mai mult, înseamnă în mod cert, că undeva, pe traseul centrală - telefon există un aparat de interceptare care consumă sau altceva care nu-și are rostul pe o linie telefonică. Dacă cumva acest dispozitiv de interceptare este pus în telefon, montând miliampermetrul într-o bornă a telefonului și firul cablului telefonic ce era legat la acesta, vom măsura cei câțiva (5-8) mA pe care-i consumă minusculul aparat de interceptare.

În concluzie, prezența unei tensiuni scăzute, sau a unui consum evidențiat cu miliampermetrul denotă, de cele mai multe ori, existența interceptării, dar viceversa, teoria nu este valabilă. Pot exista cuplaje inductive, microemițătoare alimentate cu baterii proprii, emițător de tip "infinity" neactivat și altele, care nu sunt

evidențiate prin procedeele prezentate până în prezent.

Detectarea electronică a unui emițător de interceptare a telefonului este aceeași operație ca și depistarea oricărui emițător de ascultare. Sunt însă unele deosebiri care trebuie avute în vedere. Astfel, semnalul audio care este transmis va fi furnizat de linia telefonică și nu de discuția din cameră și de aici un avantaj important pentru cel ce execută ascultarea. Aparatul de interceptare poate fi astfel plasat în telefon (de cele mai multe ori) dar și oriunde pe linia telefonică, funcție de posibilitatea de plasare a receptorului de interceptare și a magnetofonului de înregistrare, știind că distanța între acestea și emițător nu poate fi mai mare de 50 - 150 metri.

S-au reamintit aceste date, pentru că aceeași distanță (preferabil mai mică) trebuie păstrată și între locul de plasare a eventualului microemițător și dispozitivul de control. Aparatura de detectare a emițătoarelor de interceptare a convorbirilor telefonice va fi analizată odată cu cea de depistare a tuturor dispozitivelor fără fir ce interceptează și alte convorbiri, nu numai a celor telefonice, pentru că nu există nici o deosebire între ele. Totuși, va trebui să se cunoască unele lucruri, specifice acestor operațiuni de către cei care le execută. Aceste emițătoare sunt proiectate să funcționeze numai când telefonul este în funcțiune, când există un consum de cca.40 mA pe canalul telefonic iar tensiunea de la bornele liniei scade la 12 V și în linie apare semnalul electric, provocat de variațiile la presiunea acustică a rezistenței microfonului cu cărbune. De aici concluzia care se impune este că, înainte de a începe depistarea câmpului de radiofrecvență trebuie să se "provoace" o convorbire telefonică banală, care să existe în tot timpul controlului. Suntem siguri că s-a reținut de către cititori că detectarea este posibilă numai în condițiile în care aparatura de control se află în raza de acțiune a emițătorului. Controlul radio cu detectoare de câmp sau receptoare se poate completa eficient cu o inspecție vizuală a aparatului de telefon și a porțiunii accesibile de cablu, pentru a găsi eventuale modificări, piese schimbate, dispozitive ascunse.

*
* * *

Detectarea emițătoarelor "Infinity" precum și a altor sisteme de interceptare cu consumuri foarte mari pe linia telefonică, a celor care simulează "telefon ocupat" are și ea anumite particularități. Astfel, în condițiile când acestea sunt activate, deci în funcțiune, a determina prezența lor este o problemă foarte simplă. Măsurarea tensiunii la bornele telefonului când microreceptorul este pe furcă și determinarea unei valori mult mai mici decât 48 V indică prezența, așa cum am mai spus, a unui emițător "Infinity" sau a unui alt dispozitiv care interceptează discuțiile din jurul telefonului. Deoarece emițătorul "infinity" nu este activat permanent, ci pe momente operative, selectate după interesul celor ce-l activează, observarea tensiunii pe linia telefonică trebuie făcută pe o perioadă scurtă sau mai lungă de timp. S-au construit aparate destul de ieftine care realizează această supraveghere în timp și care sesizează optic sau auditiv schimbările de tensiune, ceea ce echivalează cu pornirea sau oprirea dispozitivului de interceptare. Aparat mai complicate sunt prevăzute și cu posibilitatea unui control auditiv al liniei telefonice, de ascultare a convorbirilor interceptate care sunt transmise, și de localizare astfel a încăperii unde este plasat microfonul dispozitivului de interceptare, prin compararea a ceea ce se transmite cu ceea ce se discută în diferitele camere ale locuinței sau companiei, instituției etc.

Problema complicată este activarea emițătorului "infinity". Se oferă de către producători sisteme ce generează tonuri variabile în tot spectrul audio, care vor încerca să-l pornească. Din păcate pentru cei ce execută controlul s-au realizat dispozitive "infinity" care se activează la mai multe tonuri de frecvență și tipuri de combinații între ele, fixate după un anumit algoritm care nu este ușor de descoperit.

Generatorul de ton se conectează printr-o rețea de adaptare pe linia telefonică, microreceptorul aparatului telefonic fiind pe furcă și, în caz că se reușește activarea prin trimiterea tonului sau a combinațiilor multiple dintre ele, se evidențiază aceasta prin scăderea tensiunii în jur de 12 V.

Din tot ce s-a arătat la acest capitol, credem că s-a reținut

faptul că și în condițiile când nu reușim activarea, printr-un control de mai lungă durată, cum s-a mai prezentat, se vor putea marca momentele când activarea va fi făcută de cel ce realizează interceptarea.

Când s-au tratat metodele de interceptare a convorbirilor dintr-o încăpere cu ajutorul aparatului telefonic, s-a prezentat și cea care folosește injectarea de radiofrecvență pe cablul spre aparatul telefonic din apropierea obiectivelor urmărite.

Se înțelege că aceasta poate fi pusă în evidență relativ ușor de receptoare clasice sau specializate pentru domeniul de frecvență folosit în aceste scopuri. Trebuie avut în vedere faptul că aceste măsurători, în apropierea unor stații de emisii de radiodifuziune puternice sunt îngreunate deoarece liniile telefonice se comportă, mai ales când funcționează pe porțiuni lungi pe trasee aeriene, neecranate, ca antene care captează energia de radiofrecvență. Tehnicianul care face măsurătorile pentru detectarea injecției de R.F. trebuie să interpreteze bine rezultatele, pentru a putea face distincție între cele două tipuri de radiofrecvență captate, mai ales când nu are la dispoziție aparatură sofisticată. Greutăți deosebite se pun în fața celui care odată ce a descoperit prezența câmpului de radiofrecvență în scopurile la care ne-am referit dorește să realizeze și demodularea eficientă a semnalului de radiofrecvență.

Se recomandă tehnicianului respectiv ca, odată ce este sigur că a descoperit prezența radiofrecvenței să încerce, în primul rând, să afle, pentru că nu poate fi departe (zeci de metri), locul de unde se injectează RF, și se realizează semnalul demodulat care, amplificat, poate fi trimis la câțiva km, la punctul de ascultare.

Pentru protejare împotriva RF se folosesc cu succes filtre (trece jos) care nu permit trecerea unei frecvențe peste 10 KHz. Dacă acestea sunt bine proiectate și instalate corespunzător nu deranjează funcționarea normală a telefonului și a sistemelor telefonice în ansamblu.

Abordând problema protecției împotriva oricăror dispozitive de interceptare a convorbirilor din încăperi care se folosesc de aparatul telefonic sau de cablul acestuia pe traseele din imobile ce aparțin unor instituții guvernamentale, societăți etc., trebuie să arătăm că o metodă foarte eficientă este următoarea: toate cablurile, în locul în care intră în clădire, să fie

secționare și conectate la o aparatură specială care realizează întreruperea fizică a circuitelor și reîntregirea acestora, fie prin relee fie prin alte circuite electronice. Atâta timp cât telefonul nu funcționează, circuitul lui spre centrală este întrerupt, deci orice semnal cules dintr-o eventuală interceptare nu va ieși din imobil și nu va ajunge la locul de ascultare.

În cazul în care, dinspre centrală, telefonul este apelat, primele trenuri de apel fac ca releul sau alt circuit de comutare să realizeze întregirea firului telefonic. Același lucru se obține și când se dorește o convorbire de la un telefon din clădire. Ridicarea microreceptorului este sesizată și se comandă reîntregirea circuitului care, în poziție de repaus, este așa cum am mai spus întrerupt. Cu alte cuvinte, se conectează și se deconectează de câte ori telefonul este în funcțiune, respectiv în repaus. Această aparatură este folosită deocamdată în primul rând de instituții guvernamentale, foarte vulnerabile la interceptare, în special când acestea funcționează în țări străine, ca ambasade, consulate, societăți comerciale mixte, dar poate fi folosită și de către instituții particulare care au suspiciuni serioase că telefoanele lor prezintă interes deosebit pentru concurență sau pentru alții.

Un abonat obișnuit se mulțumește cu efecte similare, poate mai puțin comode, de conectare a telefonului la rețea printr-o fișă, asigurându-și astfel o protecție în cazul când dispozitivul de interceptare este montat în telefon. Abonatul nu trebuie să uite că pentru a primi apelul telefonic trebuie să-și monteze suplimentar o sonerie, permanent conectată la rețeaua telefonică.

•
*

* *

În primele capitole ale lucrării, când au fost prezentate mijloacele de interceptare pe fir, s-au tratat și cele care folosesc microfoane cu amplificatoare care pot transmite semnalele captate, fie pe o pereche a unui cablu telefonic pe care funcționează un telefon (pe pereche ocupată), fie pe o pereche liberă. Din cele relatate până în prezent se poate deduce ușor că detectarea acestora se poate face relativ simplu când se cunoaște perechea pe care funcționează, prin ascultarea acesteia cu un

amplificator de control audio (care nu trebuie să lipsească din trusa de depistare a instalațiilor de interceptare) sau prin măsurarea curentului care alimentează amplificatorul. Probleme deosebite se pun când cablul telefonic are mai multe fire, de la 4-50 perechi și telefonul sau telefoanele pot funcționa, ca și amplificatoarele de interceptare, pe oricare dintre perechile ce se pot forma ($C^2_{\text{so}} = 1225$ perechi diferite).

Există aparatură specializată care măsoară fiecare pereche posibilă determinându-i caracteristicile în vederea depistării unor modificări la aparatele telefonice sau prezența amplificatoarelor de interceptare. Operatorul deconectează cablurile la o joncțiune sau regletă de conexiune și conectează terminalul dinspre telefon la aparatul de control, lăsând de o parte pe cel dinspre centrală. Selectarea fiecărei perechi se poate face manual de către operator sau automat, dacă instrumentul este prevăzut cu un calculator. Se înțelege că pentru a depista anumite modificări sau dispozitive de interceptare, aparatul de verificare trebuie să posede și să injecteze în perechile telefonice măsurate stimulii de funcționare a acestora care, în cazul amplificatorului la care ne-am referit, este tensiunea de alimentare 48 V deoarece cea livrată de centrala telefonică nu poate fi întrebuințată, cablul fiind în timpul testării secționat de la regletă.

Deoarece, în multe țări dezvoltate controlul instalațiilor telefonice pentru asigurarea secretului a sporit continuu s-au proiectat și realizat aparate foarte sofisticate care oferă toate posibilitățile de control la care ne-am referit până în prezent.

Aceste aparate numite testere, analizoare, detectoare ale dispozitivelor de ascultare pe linii telefonice, oferă utilizatorului toate măsurătorile ce se pot imagina și sunt necesare. Astfel, determină impedențe, capacități, rezistențe, precum și tensiuni și curenți în cele două situații (telefon închis sau deschis), introduc tonuri vocale sau combinații ale acestora pentru activarea dispozitivelor "infinity", realizează "ascultarea" liniilor pentru depistarea microfoanelor cu amplificatori. Cele mai perfecționate dintre acestea pot detecta și injectările de radiofrecvență și dispozitivele care folosesc curenții purtători până la 300 KHz, au o sensibilitate în jur de 100-150 μV și posibilități de ascultare a modulației de amplitudine, de frecvență și a transmisiunilor cu o singură bandă laterală.

Se înțelege că se poate executa automat cu astfel de

aparate și măsurarea celor 1225 de combinații de perechi posibile ale unui cablu de 50 de perechi, așa cum s-a descris mai înainte.

Un astfel de aparat-tester computerizat, fabricat de CCS, firmă la care ne-am mai referit, denumit CCTA 1000, este montat într-o servietă tip diplomat, cu afișare a măsurătorilor pe care le efectuează și rezultatele acestora, cu comandă pe bază de microprocesor, cu programare internă a procedurilor de testare. În prospectul aparatului CCTA 1000 se folosesc expresii de forma: "Intrarea în perioada secretului computerizat", "CCTA este un sistem de căutare specializat care conduce la localizarea dispozitivelor de interceptare ascunse (hidden eavesdropping divices) în auto, locuință, birouri", "CCTA face toate operațiile pentru detectarea și fixarea cu precizie a aparaturii de interceptare din sistemele telefonice". Lăsând la o parte reclama, trebuie să recunoaștem că acest instrument, care costă 15000 dolari S.U.A., este deosebit de eficient în scopurile pentru care a fost creat.

Un aparat asemănător a fost conceput și realizat în țară în două variante constructive, pentru export dar și pentru unele nevoi interne speciale, la o treime din prețul celui produs de firma CCS, cu aproximativ aceleași funcțiuni și posibilități de cuplare la un oscilograf, pentru vizualizarea spectrului de frecvențe analizat, cu anumite minusuri față de CCTA 1000 în domeniul computerizării și automatizării operațiunilor dar cu rezultate finale foarte asemănătoare.

Complexitatea aparaturii folosite solicită cunoștințe tehnice, în telecomunicații și electronică și o bogată experiență din partea operatorului. Durata unui control asupra unui telefon cu cinci butoane poate fi, chiar cu aparatură automatizată, între 30-60 minute. Iar o oră de lucru, în acest domeniu al depistării tehnicii de interceptare poate fi evaluată, în funcție de aparatura folosită, de tehnicitatea echipei și garanțiile acordate în urma controlului, în jur de până la 1000 dolari S.U.A.

**Mai bine cauți un ac în carul cu fân
decât un microfon într-o clădire**

Până în prezent, s-au abordat problemele tehnicii de depistare având la dispoziție cablurile telefonice, cel puțin pe porțiunea din imobil sau împrejurimile acestuia și aparatele de

telefon existente într-o încăpere, birou, instituție etc.

Să ne imaginăm că ni se cere și este necesar să depistăm într-o încăpere, apartament, clădire, microfoane cu amplificatoare și nu cunoaștem locul și traseul pe care le parcurg firele acestora până întâlnesc un cablu telefonic, și că nu avem acces la el. Rezultatul investigației, care seamănă cu o operație de căutare a acului în carul cu fân, depinde în primul rând de experiența, perseverența și meticulozitatea echipei de tehnicieni precum și de aparatura pe care o au la dispoziție. Sunt așa de multe operații, așa de multe specialități și cunoștințe necesare pentru membrii grupei de control pentru a depista dispozitivele de interceptare pe fir, dacă bineînțeles acestea există, încât ne-ar trebui un spațiu foarte mare pentru a trata exhaustiv aceste probleme și, de aceea, ne vom limita la a prezenta metodele și principiile generale, precum și aparatura principală necesară acestui control.

Totul trebuie început cu o inspecție vizuală a locurilor unde ar putea fi plasat microfonul, să se descopere orificiul cu diametru de câțiva milimetri necesar pentru ca acesta să poată capta convorbirile și traseul unde au fost pozate cablurile de microfon, pentru a prelua și alte dispozitive de interceptare și apoi pentru a ieși din apartament. De obicei, microfoanele se plantează cât mai aproape de locul unde au loc discuțiile, la îmbinările dintre ziduri și podele, lângă calorifere, tocul ușilor sau ferestrelor, lângă prize etc. De regulă, nu se vor plasa, deci nici nu se vor căuta în pardoseli, când acestea sunt acoperite cu gresie sau linoleum și nici în porțiunile centrale ale încăperii, indiferent din ce este făcută pardoseala, deoarece acestea sunt, de multe ori, acoperite cu covoare, mochete, preșuri etc. și nu mai poate avea loc captarea sunetului.

Dispozitivele de interceptare cu fir nu se caută în mobilă și alte obiecte din camere, pentru simplul motiv că nu pot fi montate în acestea, deoarece ele se pot muta și astfel se descoperă cablul cu care sunt conectate.

Inspecția vizuală urmărește să evidențieze, în primul rând, lucrări noi executate (necesare plasării și mascării dispozitivelor de interceptare) pentru că, oricât de bine și atent ar fi fost făcută operația de montare a unui microfon, amplificator sau a unui cablu, se pot evidenția deosebiri de material folosit, de culoare față de vechea zugrăveală, mai ales dacă aceasta este foarte veche. Spre exemplu, dacă s-a făcut un locaș în perete, pentru a

plasa microfonul sau un traseu pentru a poza o pereche de fire, acestea nu se mai refac cu mortar, cu ciment, ci cu ipsos rapid pentru a se usca foarte repede și a face corectura de culoare.

Dacă la lumina zilei, cu ochiul unui specialist nu se pot evidenția deosebirile, se folosește lumina ultravioletă care pune în evidență, fără greș, porțiunile în care s-au executat lucrări noi de tencuială și zugrăveală. Acestea apar cu fluorescență diferită față de porțiunile unde nu s-au făcut retușuri și sunt așa cum au fost executate de la ultimele lucrări de întreținere a încăperii. De aici concluzia că cel mai greu de depistat sunt instalațiile de interceptare ce s-au executat odată cu lucrările de zugrăveală și vopsitorie generale ale imobilului.

Controlul vizual poate fi completat, în afară de lampa UV, la care am făcut referire și cu detectorul de metale care ne poate fi de mare ajutor, deși el semnalizează și alte obiecte metalice. Acesta este și motivul pentru care dispozitivul de interceptare se plasează, de multe ori, lângă obiecte metalice sau în spatele acestora.

În general, se întulesc și se exclud de la controlul distructiv traseele cu cabluri electrice care sunt îngropate sub tencuiala zidurilor, de regulă, între dozele electrice, între acestea și prize, ele fiind orizontale în apropierea tavanului și verticale până la prizele electrice. Detectarea prezenței altor trasee în care se află metal (fire metalice), în special la îmbinările dintre pereți, ziduri și planșee, pune semne de întrebare care necesită răspunsuri și lămurirea scopului pentru care au fost pozate aceste cabluri.

Detectorul este util și la controlul obiectelor din lemn (ferestre, uși), în porțiuni unde se știe că nu există cuie, balamale, forăibere etc.

Un aparat deosebit de util, folosit la început în scopuri guvernamentale, în special în S.U.A., de către F.B.I. și de cei ce asigură protecția Casei Albe, este aparatul portabil cu raze X, în greutate de max. 20 kg și care costă în jur de 2000 dolari S.U.A. Pentru început, el s-a folosit la controlul nedistructiv al pachetelor, obiectelor de artă, a obiectelor suspecte a fi folosite în scopuri teroriste pentru ca apoi să se extindă la vizualizarea planșeelor, a pereților, pe ecrane fluorescente sau fotografii. Sigur, el se folosește pentru explorarea unor porțiuni devenite suspecte ca rezultat al folosirii altor metode, când se dorește un nou control

înainte de deteriorarea porțiunii respective, în general greu de refăcut.

Evidențierea conturului dispozitivului ne dă o certitudine asupra naturii acestuia.

Este de la sine înțeles că acest aparat nu este la îndemâna oricăror echipe de depistare, necesită unele precauțiuni, cunoștințe și riscuri pentru operator. În domeniul depistării tehnicii de interceptare, acesta a fost înlocuit parțial de alte tehnologii și sisteme deosebit de eficiente.

Este vorba de tehnologia detectării joncțiunilor neliniare care a fost dezvoltată în ultimii ani la cererea Guvernului federal al S.U.A., pentru cercetări de detectare a armamentului. Ea a fost perfecționată și s-a stabilit că poate fi folosită și în detectarea circuitelor electronice ce conțin tranzistoare, diode, circuite integrate care, la rândul lor, sunt formate din semiconductori, din joncțiuni neliniare.

Cum toate amplificatoarele, microemițătoarele și alte dispozitive de interceptare sunt construite din aceste componente electronice, se înțelege că, detectându-le pe acestea, punem în evidență întregul dispozitiv de interceptare, scopul controlului nostru.

Aparatul respectiv utilizează o tehnologie sofisticată și injectează printr-o antenă de construcție specială, adecvată scopului propus, un câmp de frecvență din domeniul VIF.

Semnalul radio este receptat de montajul electronic cu semiconductori. Acesta, prezentând caracteristici neliniare de răspuns, face să apară o anumită armonică, proprie joncțiunilor cu semiconductori, a semnalului receptat, care este retransmis și captat de receptorul care se găsește ca parte componentă a aparatului de depistare a joncțiunilor neliniare. Leșirea receptorului este prevăzută cu unul sau mai multe instrumente de măsură pentru a arăta intensitatea semnalului captat.

Aceste aparate sunt foarte eficiente pentru scopul arătat până la o distanță de 9-10 m, dar foarte costisitoare (15-20 mii dolari S.U.A.). Ele necesită o pregătire serioasă a operatorului pentru a putea identifica răspunsul joncțiunilor dispozitivelor electronice ascunse și nu a radioreceptoarelor portabile, televizoarelor, magnetofonelor aflate în apropiere, dar la vedere, sau de joncțiunile primite de la obiecte metalice oxidate aflate în zona de detectare. Bineînțeles că în cazul unor dispozitive bine

ecranate răspunsurile sunt mici și se întrevăd greutăți la evidențierea lor dar sistemul prezintă un avantaj deosebit deoarece el detectează instalații de interceptare care, în prealabil, nu trebuie să fie activate sau alimentate.

Se detectează simpla lor prezență și nu efectele punerii lor în funcțiune (câmpuri, semnale vocale, curenți, tensiuni etc.).

Este, așa cum am mai spus, un aparat deosebit de perfecționat, scump, dar eficient pentru a descoperi tehnică electronică ascunsă, care s-a fabricat atât în străinătate, cât și în țară, cu precădere pentru sarcini de export.

Dar, să facem un salt de la cea mai complexă metodă la o alta pentru a ilustra rolul ingeniozității și experienței operatorilor și tehnicienilor care execută controlul în vederea depistării tehnicii de interceptare și nu numai a importanței aparaturii și să relatăm următoarele:

Un tehnician electronist român a depistat, cu mulți ani înainte, un microfon într-o clădire în care funcționa o instituție a statului român dintr-o țară străină, folosind un simplu ac de găsmălle, legat la un capăt de o ață subțire și lăsat vertical în imediata apropiere a peretelui. Nu mică i-a fost surprinderea când, repetând de câteva ori această operație, tot de atâtea ori acul era deviat de la poziția verticală și era atras și lipit de zid. S-a presupus și s-a dovedit că magnetul permanent al unui microfon ascuns "era vinovat" de aceasta.

Activitatea de depistare a instalațiilor de ascultare cu fir este o treabă deosebit de grea și este mai costisitoare decât cea de control a instalației telefonice. În urma controlului, pentru o siguranță mai mare că nu vor exista sau n-au fost instalații de interceptare, în timpul acestei activități, se ajunge de multe ori la deteriorarea unor mari porțiuni din tencuiala pereților sau scoaterea unor importante porțiuni din parchet, în special a zonelor din apropierea pereților.

De aici concluzia că, în trusa de căutare, pe lângă aparate perfecționate, trebuie să se găsească multe scule de ciocănit, spart, îndoit, precum și cele necesare refacerii încăperilor așa cum au fost înaintea controlului.

În unele situații, dacă clădirile au fost mult timp la dispoziția celor ce sunt suspectați că execută interceptarea sau în cazurile în care în camerele unui imobil se discută lucruri deosebit de secrete, controlul poate începe prin executarea (dacă este

posibil și permis) unui șanț de adâncime de 1-1,5 m în jurul clădirii, pentru a descoperi eventuale cabluri prin care sunt transportate semnalele interceptate spre centrul de ascultare. Pornind de la eventualele cabluri descoperite este numai o chestiune de timp pentru a ajunge la microfon.

•

• •

Cu toate acestea, nu înseamnă că orice fir descoperit conduce neapărat la o instalație de interceptare. Acest adevăr precum și poveștile răspândite în presa română de unii ziariști în legătură cu descoperirea de microfoane în telefoane, după calorifere, în candelabre și chiar sub covoare (probabil nu s-a măturat de mult timp) face interesantă relatarea apărută într-o publicație bucureșteană în 1993, sub titlul "Microfonul de sub covor" și pe care autorul prezentei lucrări o consideră autentică și relevantă, și de aceea se redă în continuare aproape așa cum a apărut:

"Intr-o după amiază, în anul 1966, după orele de program sunt anunțat să mă prezint urgent la ministrul de interne Cornel Onescu (acesta îl înlocuise pe Alexandru Drăghici odată cu "promovarea" lui, după congresul al IX-lea din anul 1965, ca secretar al CC al PCR). Solicitățile de prezentare la ministru nu erau fapte obișnuite și de aceea am căutat să mă gândesc ce s-a putut întâmpla, pentru că știam că nu sunt chemat să fiu felicitat. La sosire nu m-a lăsat să mă prezint și m-a atacat direct:

- Voi puneți microfoane și ascultați conducerea partidului?

M-am liniștit văzând că este vorba de o năzbâtie, nimic serios și am căutat să-l conving că așa ceva nu este posibil. A continuat și mi-a spus că a fost sunat de Virgil Trofin, proaspăt secretar al C.C.-ului, care după ce s-a mutat într-o casă nouă a găsit "urme" ale unei instalații de ascultare, microfoane sau ceva asemănător - spusele lui fiind neclare. Totodată, Virgil Trofin i-a reproșat ministrului și faptul că subordonații lui lucrează prost și lasă urme grosolane, pe care le-a observat cu ușurință. Am încercat să explic din nou illogicul acestor acuzații, dar am fost oprit și după ce mi s-a dat adresa lui V.T., (undeva în cartierul Piața Victoriei și Dorobanți) mi-a ordonat să mă prezint la acesta

și să lămuresc problema, pentru că altfel ne va reclama secretarului general Nicolae Ceaușescu. Eram conștient de gravitatea situației, pentru că realizam că, neputând să-l conving pe ministru, cu atât mai greu va fi să-i explic lui V.Trofin.

La început s-au verificat evidențele, s-au consultat colaboratorii pentru a se afla ce s-ar fi putut întâmpla. S-au analizat toate ipotezele. Nu s-a exclus nici ideea ca situația creată să fie opera unui serviciu de spionaj străin. La fel era posibil să fie o instalație veche și uitată de către noi. Indiferent cine erau autorii acestei tehnici de interceptare, realizam că tot noi lucrătorii din tehnica-operativă eram vinovați.

Am devenit mai calm când am aflat că timp de câteva luni de zile casa a fost la dispoziția gospodăriei de partid, care prin întreprinderile sale de construcții a reparat-o, modernizat-o, a zugrăvit-o, a rașchetat parchetul și a reparat instalațiile electrice, sanitare etc. Mi-am dat seama că dacă ar fi existat tehnică de interceptare, aceasta ar fi fost descoperită de constructori sau de instalatori, iar eventualele urme ar fi fost șterse. Am plecat la adresa ce mi se dăduse și m-am trezit în fața unei case cu parter și etaj și cu o mică curte în jurul ei. Deoarece nu mi s-a răspuns la încercările de a intra prin ușa principală, am fost obligat să mă folosesc de cea din spate, pe care găsim-o deschisă, am urcat până la etaj. Casa scării era îngustă, în dreapta se afla viitoarea sufragerie, care nu era complet mobilată, iar în stânga bucătăria și cămara. M-a primit V.Trofin, care de la început mi-a făcut observația că lucrăm prost și cu un gest teatral a apucat un colț al covorului și dându-l la o parte a lăsat să se vadă o porțiune de parchet. A continuat răstit: 'Ce-i cu porcăria asta?'... Într-adevăr, în parchet era prevăzut un locaș special, frumos construit, acoperit cu un căpăcel rabatabil din alamă și din care ieșeau două fire subțiri în lungime de câțiva metri. Sigur că acestea se vedeau deoarece erau plasate în mijlocul camerei și ele constituiau <<urmele>> descoperite de V.T. și motivul intervenției lui la C.O.

Mi-au trecut emoțiile și, explicându-i condescendent, dar în același timp, așa cum se spune de sus, cum o fac cei stăpâni pe situație și anume, că în toate <<casele mari>> sunt prevăzute astfel de instalații în sufragerii, firele fiind pozate de constructor ca să fie legate la un buton de sonerie care să stea sub covor, plasat de regulă sub o masă, pe care se servesc

bucatele. Când se dorește să fie chemat valetul, chelnerul sau femeia de serviciu, stăpânul sau stăpîna casei, în mod discret, apasă butonul soneriei de sub covor. M-a ascultat atent, la început a fost descumpănit dar nu a cedat și mi-a cerut să-l fac demonstrația. Mi-au revenit emoțiile pentru că deși eram sigur că aveam dreptate, nu cunoșteam dacă întreaga instalație era în funcțiune deoarece butonul nu era pozat și nu știam dacă era montat clopoțelul.

Am dezizolat capetele firelor și le-am scurt-circuitat. Un zgomot puternic care mi s-a părut cel mai cristalin și muzical sunet pe care l-am auzit, anunța că experiența reușise și că soneria funcționa. Virgil Trofin a pus covorul la loc, astupând astfel firele, vădit incomodat și stânjenit. ..."

Întrerupem aici relatarea, ea neprezentând în continuare interes pentru ce ne-am propus. Tot așa pot sta lucrurile și cu "microfonul găsit sub covor" de către ziariștii-filologi căutători de instalații de ascultare. Dar dacă V.Trofin avea acum aproape 30 de ani circumstanțe atenuante pentru că nu era prea școlit, umblat, nu văzuse prea multe "case mari", nu aceleași circumstanțe putem să le acordăm ziariștilor noștri, care au cel puțin pretenția de oameni cu multiple cunoștințe.

Prin această relatare vrem să arătăm că psihoza ascultării convorbirilor în țara noastră nu este nouă și că ea a existat atât înainte cât și după 1989, că istoria se repetă schimbându-se doar actorii și că depistarea instalațiilor de interceptare nu este o treabă de amatori.

*

* *

Intr-un studiu făcut în străinătate s-a concluzionat că, asemănător multor domenii de activitate, organizațiile prestatoare de servicii în acest segment al contramăsurilor sunt foarte diferite.

Referindu-ne la S.U.A., putem spune că unele dintre acestea și mai ales cele constituite prin diferite agenții de către guvernul federal, precum și cele în care activează cadre pregătite sau care au făcut parte din acestea, sunt caracterizate prin competență, seriozitate și înalt profesionalism. Altele, din păcate și cele mai multe, sunt interesate în primul rând în câștiguri ușoare

și dau garanții nefundamentate.

Cei care solicită astfel de servicii trebuie să știe că, după executarea unui control complex, deoarece se plătesc sume importante, trebuie să ia măsuri ferme de pază și alarmare, pentru a preveni noi pătrunderi în vederea introducerii unor noi dispozitive de interceptare.

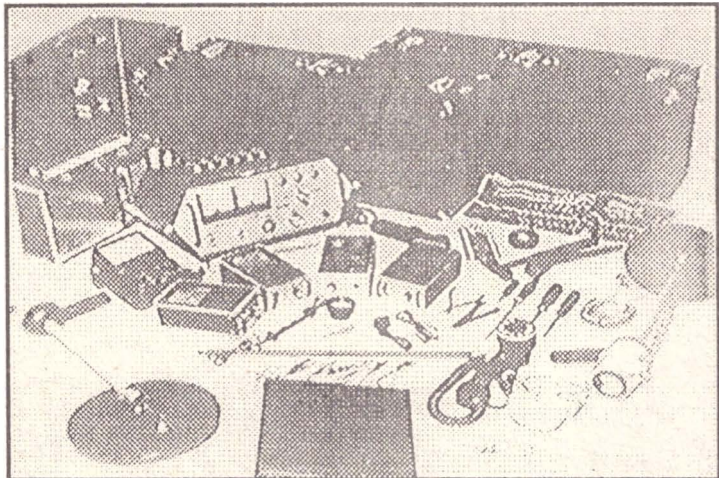
*

* *

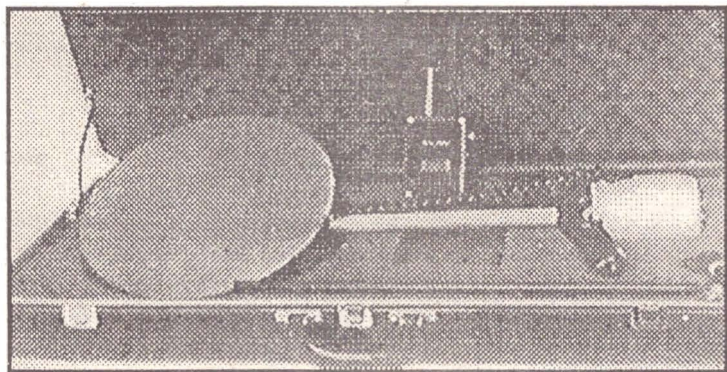
Cititorii trebuie să știe că toate serviciile de contrainformații ale statelor dezvoltate dispun de echipe de control formate din specialiști cu multă experiență care se ocupă de depistarea eventualelor tehnici de interceptare montate clandestin în ambasadele și locuințele diplomaților lor din aproape toate capitalele țărilor lumii. Sigur că în timpul războiului rece echipele de control ale C.I.A. acordau, spre exemplu, în primul rând atenție ambasadelor S.U.A de la Moscova, Berlin, Praga, Budapesta, Varșovia etc. Înaintea celor de la Nairobi, Brazzaville, Lagos, dar fără să le negligeze pe cele din Londra, Paris, Stockholm etc. Așa se explică de ce, cele mai multe tehnici descoperite s-au produs în ambasade, consulate, reședințe.

Relatăm în continuare, pentru a înțelege mai bine ce înseamnă dotarea și profesionalismul unora din aceste echipe, un fapt întâmplat în București prin anii '70. În clădirea anexă a unei importante ambasade ce aparținea unei mari țări occidentale, europene, în care funcționa atașatura ei militară și serviciul de cifru, erau montate trei microfoane de contraspionajul român. Acestea au fost introduse din exteriorul clădirii, prin calcanul ei, care era accesibil numai din curtea unei alte locuințe, ce nu aparținea ambasadei.

Este de la sine înțeles că pentru echipa de control acest zid exterior constituia partea căreia trebuia să i se acorde cea mai mare atenție. Profesionalismul și dotarea lor, care trebuie evidențiate, au rezultat din faptul că au controlat din interior un zid exterior în suprafață de cca 160 m² și au dat înspre exterior numai trei găuri exact în locurile unde erau plasate microfoanele (nici una în plus, nici una în minus) pe care le-au scos.



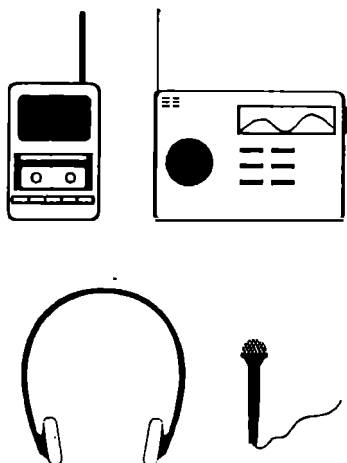
Aparatura si scule din trusa obligatorie a celui care depisteaza dispozitive de interceptare.



Detector de metale.

Trebuie să recunoaștem că este o performanță care nu stă la îndemâna oricărei echipe de control. Pentru a fi exacti trebuie să spunem că foarte multe echipe de control ce încercau depistarea tehnicii operative au "trecut" peste instalațiile de ascultare și le-au lăsat în funcțiune. Cele mai multe erau însă scoase din funcțiune înaintea începerii controlului și repuse după plecarea echipei de control. La o altă ambasadă din București, tehnica introdusă a fost descoperită după executarea șanțului din jurul clădirii la care m-am referit.

Lupta dintre echipele care montează microfoane și cei care le caută s-a dus pe multiple planuri și nu de puține ori se plasau instalații de interceptare care erau, prin modul cum au fost executate, oferite celor ce le căutau tocmai pentru a salva pe cele care erau instalate în paralel, după toate regulile și care funcționau în continuare, cu rezultate operative deosebite pentru că aceia care erau urmăriți nu se mai fereau, după "reușita" echipei lor de control.



CAPITOLUL XIV

DETECTAREA DISPOZITIVELOR DE INTERCEPTARE RADIO (FĂRĂ FIR)

Până aici, ne-am referit numai la depistarea instalațiilor de ascultare clandestine care își transportă semnalele culese pe cabluri telefonice sau alte fire special pozate.

Dar, după cum se cunoaște, odată cu prezentarea mijloacelor ofensive, s-au descris și microfoanele (microfoane - fără fir) de diferite tipuri de modulație și protecție contra depistărilor, care sunt pornite sau oprite de la distanță la dorință și care sunt mult folosite fiindcă sunt mult mai ușor de plasat decât cele cu fir. În cele ce urmează, ne vom ocupa de depistarea acestora și, încă de la început, trebuie spus că această operație, dacă este făcută cu aparatură profesională iar rezultatele controlului (testelor) sunt interpretate corect, este mult mai ușoară și cu finalitate mai sigură decât cea privind depistarea microfoanelor cu fir. Pentru o înțelegere mai ușoară, vom prezenta mijloace și aparatură de la cele mai simple până la cele mai sofisticate. Nu este însă obligatoriu ca în activitatea de control să se respecte această ordine în folosirea mijloacelor respective.

Cel mai simplu instrument este măsurătorul sau detectorul de câmp care indică prezența și cuantifică intensitatea energiei de radiofrecvență prezentă, la un moment dat, într-un punct al spațiului. Aparatul este format dintr-o antenă (de obicei telescopică), o diodă detectoare, un amplificator cu sensibilitate reglabilă, din dispozitive acustice, luminoase și un instrument pentru măsurarea energiei de radiofrecvență existentă.

Este descrierea faimosului "Bird" care a făcut multă vâlvă, în primăvara anului 1993, în unele ziare românești și cu care s-a pretins că s-au descoperit microfoane în unele instituții importante și în locuințele unor oameni politici. Este exemplul clasic când un instrument cu anumite posibilități și limite intră pe mâna unor operatori fără cunoștințe tehnice, dornici de senzațional, scandal, de reclamă exagerată și cu orice preț a aparatului etc. În cele ce

urmează vom vedea performanțele acestuia și vom sesiza și aberațiile care s-au putut vehicula în presă pe seama lui. Poate că nu mai abordam această problemă dar, în iunie '93, din nou aceleași ziare, cu alte semnături, reiau discuția asupra "Bird-ului" descoperind "burlane" vorbitoare în casa unui viceprimar (!).

Detectoarele de câmp au cunoscut îmbunătățiri continue în sensul că s-au creat posibilitățile de acord, în care banda de frecvență este împărțită în subbenzi mai mici, pentru a permite o amplificare separată a câmpului, în game de frecvență distincte. De asemenea, s-au construit detectori cu montaje pe două circuite de măsură și o antenă duală ce acționează diferențial. O parte a antenei, fiind mai aproape de microemittătorul clandestin, va primi o cantitate de energie mai mare decât cealaltă care este mai depărtată. Diferența de intensitate se evidențiază numai dacă câmpurile sunt mici și o antenă este mai aproape decât alta față de sursa de câmp electromagnetic iar diferența între detector (câmpometru) și emittător este de câțiva metri.

Se înțelege ușor că o anumită diferență de 20 - 25 cm între cele două antene nu contează când se măsoară câmpul unui emittător puternic, plasat la sute de metri sau kilometri. De aceea, perfecționarea este menită tocmai să înlătore influența acestor câmpuri puternice de la posturile locale de radiodifuziune, care prezintă practic același câmp în ambele antene ale detectorului.

La cele mai noi tipuri s-a încercat și demodularea semnalului la ieșirea măsurătorului de câmp pentru a se putea asculta semnalul audio transmis și a ajuta astfel la localizarea acestuia, fără ca cel care interceptează să sesizeze controlul. Astfel intrăm însă pe nesimțite în domeniul receptorului pe care-l vom trata ceva mai departe.

Cu toate perfecționările aduse, câmpometrele prezintă dezavantajele detecției cu diodă de bandă largă care captează atât câmpurile puternice ale stațiilor de televiziune, cât și ale celor de radiodifuziune, ale stațiilor de radio portabile și fixe pentru poliție, salvare, taxi.

Operatorii care lucrează cu astfel de aparate cunosc că intensitatea măsurată a unui câmp electromagnetic poate varia într-o încăpere și din cauza undelor staționare și a apropiării de cablurile electrice sau de alte fire și aparate telefonice care joacă rol de antenă pentru captarea câmpului exterior, informații tehnice pe care ziariștii care au lucrat cu "Bird-ul" nu le cunoșteau sau

n-au vrut să țină seama de ele.

Aceste aparate care evidențiază câmpurile electromagnetice și nu microfoane sau amplificatoare (cum s-a afirmat în presă), au o anumită importanță în domeniul contramăsurilor, realizează un test ajutător, pun la dispoziție o probă suplimentară dar nu pot constitui, din cauza limitelor lor, instrumente principale de detectare și localizare a emițătoarelor de mică putere, mai ales când asupra acestora s-au luat unele măsuri de protecție.

Emisiunile dispozitivelor de interceptare sunt captate la punctele de ascultare cu receptoarele. Este normal ca în acțiunea de depistare și localizare a acestora să se folosească tot acestea ca instrumente principale. Desigur, nu este vorba de receptoare de radiodifuziune standard, comerciale, chiar dacă ele ar mai avea în afara de UL, UM, FM, unele benzi radio rezervate poliției sau serviciilor guvernamentale, ci de receptoare special destinate acestui scop. De regulă emițătoarele sunt construite pe frecvențe în afara celor rezervate radiodifuziunii, din motive lesne de înțeles.

Receptoarele de supraveghere, de contramăsuri sau contrainformații cum se mai numesc, trebuie să aibă o înaltă sensibilitate, având în vedere puterea redusă a microemițătorului, o bună selectivitate pe un spectru larg de frecvență și posibilitatea de a recepționa semnale de diverse tipuri de modulație. Ele trebuie să dispună de stabilitate în frecvență și de o puternică rejecție a semnalelor nedorite din canalele de frecvență adiacente.

Aceste caracteristici, la care se adaugă și o lățime de bandă mai mare pentru a permite recepționarea transmisiilor ascunse cu subpurtătoare nu se regăsesc la receptoarele FM clasice, comerciale. De aceea, pentru scopul la care ne referim s-au proiectat și realizat instrumente speciale, fie că sunt manuale, automate, portabile sau staționare, cu sau fără adaptor panoramic pentru a vizualiza emisiunile captate.

În proiectarea receptoarelor speciale pentru contramăsuri trebuie să se elimine inconvenientul receptoarelor comerciale FM cu circuit de reglaj automat al frecvenței (RAF), care le împiedică să se acorde pe semnale de putere mică, când frecvența emițătorului de interceptare este aleasă voit în apropierea unui post FM de radio - difuziune locală. Receptoarele staționare cu căutare automată asigură baleierea de la 2 MHz până la 2 - 4 GHz, înregistrează fiecare emisiune captată după care pleacă mai

departe pentru parcurgerea întregii game, afișează digital frecvențele pe care se acordă etc. Se pot proiecta cu memorie, pentru ca posturile cunoscute de radiodifuziune să poată fi eliminate de la control, oprire și înregistrare.

Cele mai sofisticate sunt prevăzute și cu sonar și corelator pentru localizarea microfoanelor fără fir. Pe lângă aceste receptoare sofisticate care costă aproximativ 100000 dolari S.U.A., realizate pentru scopuri speciale, și în țară există receptoare portabile cu performanțe foarte bune care acoperă o gamă de la 50 MHz la 0,5 - 1 GHz în 4 - 5 subgame cu sensibilitatea variind de la 10 - 200 μ V în funcție de subgama în care se lucrează, cu antene telescopice a căror lungime este bine să fie reglată funcție de banda de frecvență explorată.

Pentru a reduce costul de producție al acestora se recomandă cumpărarea, transformarea și îmbunătățirea performanțelor receptoarelor comerciale, mai ales când este vorba de o serie mică, pentru că se pot folosi majoritatea părților mecanice și foarte multe din circuitele lor electronice. Suntem convinși că s-a reținut din primele capitole că fabricanții de emițătoare de interceptare pentru a le masca și proteja folosesc o modulație netradițională - așa numita tehnică a subpurtătoarei.

Semnalele de la aceste emițătoare cu subpurtătoare sunt în afara benzii radioreceptoarelor clasice și nu pot fi demodulate ușor. Ele pot fi, totuși, depistate în mod vizual cu un analizator de spectru, la care ne vom referi mai târziu sau cu un receptor prevăzut cu afișaj panoramic.

Pentru ascultarea semnalului audio, receptoarelor le sunt necesare două procese de detecție. În cadrul primului, are loc detecția semnalului principal de înaltă frecvență de regulă în unde metrice sau diametrice (VHF sau UHF) și această operație dă posibilitatea să se "prelucreze" cea de-a doua frecvență (subpurtătoarea) în unde kilometrice sau mai mari (VLF sau LF unde lungi sau foarte lungi) și să se obțină în final semnalul audio.

Dacă frecvența principală a emițătorului cu subpurtătoare este recepționată cu un aparat clasic, fără a întreprinde nimic pentru cea de-a doua detecție, semnalul de la ieșire va fi foarte slab și practic nu se va auzi nimic.

Deși în aparatura profesională destinată scopului la care ne referim, pentru cea de a doua detecție, așa numitul receptor VLF (foarte joasă frecvență) este înglobat, realizând un aparat cu

funcții complexe, unii producători l-au realizat pe acesta din urmă și în formă constructivă separată de dimensiuni mici, ușor transportabil, destinat să lucreze fie împreună cu un receptor care detectează frecvența purtătoare primare, fie pentru scopuri la care ne vom referi în continuare. Aceste receptoare VLF, destinate radio-filajului, trebuie să aibă o sensibilitate bună pentru a putea fi posibilă detectarea emisiunilor de mică putere, o selectivitate adecvată și o acoperire a gamei de frecvență între 10-300 KHz sau chiar până la 500 KHz. Ele pot fi folosite și pentru detectarea sistemelor de interceptare care transmit pe linii telefonice informațiile obținute nu în banda audio ci ULF. Se pot intercepta aceste semnale și în apropierea cablului dar cele mai bune și sigure rezultate se obțin dacă printr-o rețea de adaptoare se cuplează receptorul VLF direct pe perechea de fire telefonice sau de ce nu, electrice, pentru că s-a reținut că interceptarea folosind principiul sistemului de curenți purtători se folosește și pe aceste cabluri pentru a ieși comod dintr-un imobil.

Receptoarele de supraveghere descrise sunt în măsură să localizeze și să identifice toate emițătoarele clandestine, bineînțeles în afara celor care funcționează pe o frecvență care nu se găsește în gama receptorului sau a celor care sunt prevăzute cu telecomandă și în momentul controlului sunt în repaus, deconectate.

Instrumentele de depistare trebuie utilizate cel puțin cu aceeași iscusință de care au dat dovadă cei care au proiectat emițătorul de interceptat și cei care l-au ascuns.

Controlul cu această aparatură trebuie făcut, dacă nu permanent cu receptoare automate, cel puțin periodic, având în vedere ușurința cu care se poate plasa un dispozitiv de interceptare fără fir. Audiențele, conferințele de presă, recepțiile, o vizită oarecare, fără să mai vorbim de pătrunderile secrete sunt tot atâtea posibilități ca acesta să fie plasat chiar în prezența celui care va fi ulterior ascultat. Dacă nu permanent, cel puțin înaintea unor reuniuni importante (conferințe și congrese de partid, consilii de administrații, ședințe de redacție etc.) sau după anunțate vizite ale unor persoane suspecte, este necesar să se realizeze controale cu receptoare specializate.

Același tehnician care a relatat despre depistarea unui microfon cu ajutorul unui ac de gălălie a afirmat că, pentru localizarea într-o clădire, proprietate a statului român dintr-o țară

a Orientului Apropiat, i-au trebuit câteva zile de așteptare, de căutare cu receptoare de contramăsuri specializate, pentru a depista momentul când cele câteva emițătoare alimentate la rețea au fost pornite pentru a le putea localiza. În ultimii ani, analizatorul de spectru a câștigat un loc bine meritat în tehnica depistării dispozitivelor electronice fără fir datorită posibilităților pe care le oferă de a se vizualiza procesele de modulație sofisticate.

Această capacitate de a afișa emisiuni pe o largă porțiune din spectrul radio, deci și a benzilor laterale ce conțin informația audio, compensează în unele situații sensibilitatea mai redusă a acestora față de receptoare.

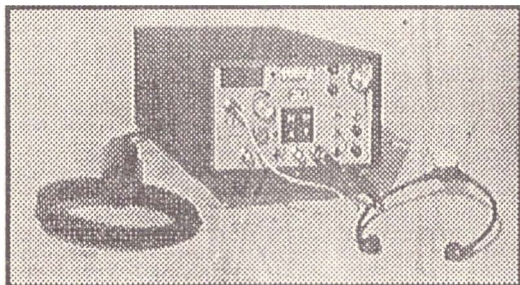
Ultimele tipuri de analizoare de spectru pot să varieze lărgimea benzii de frecvență, pentru receptarea neperturbantă a transmisiilor și prin folosirea unor tuburi de remanență pot depista prezența emițătoarelor cu salturi de frecvență sau a dispozitivelor cu spectru distribuit. În ultimii ani, acestea s-au realizat la dimensiuni mici, variante portabile, la prețuri între 5 - 10000 dolari S.U.A. Analizorul poate fi considerat ca un aparat complementar al receptoarelor, care mărește posibilitățile unei echipe de inspecție de a identifica semnalele ce nu pot fi detectate de receptoare.

În acest caz, operațiunea de căutare este recomandabil să fie făcută folosind la început analizorul de frecvență, pentru vizualizarea emisiunii clandestine și apoi inspecția trebuie continuată cu receptoare specializate pentru detectarea semnalului audio.

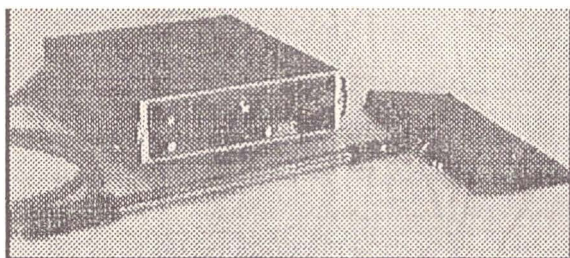
*

* *

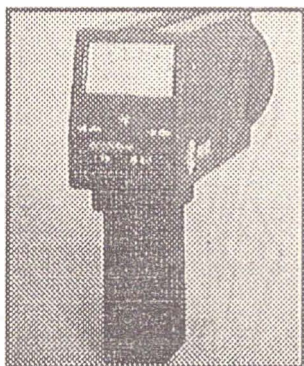
Pentru a depista prezența fasciculelor de microunde cum sunt denumite undele decimetrice și chiar centimetrice care provin de la un microemițător ascuns, cu frecvența în acest domeniu fie, foarte probabil de la o sursă exterioară pentru a activa dispozitivele pasive, s-au proiectat și realizat instrumente specializate denumite după scopul pentru care au fost construite, detectoare de fascicule cu microunde (microwave radiation detector). Deoarece trebuie evidențiate emisiuni de câțiva GHz și având în vedere caracteristica de propagare a acestora (fascicule)



Analizor linii telefonice



Detector de jonctiuni neliniare.



Detector de fascicole
cu microunde.

ne imaginăm ușor că aparatele de detectat trebuie să fie și ușor de manevrat, pentru a putea plasa antena aparatului pe direcția fascicolului. Cel mai răspândit sistem de acest tip este construit sub forma unui aparat de filmat sau, mai modern, a unei videocamere. În locul obișnuit al obiectivului se află antena, compactă, cu un câștig de 4 - 6 dB și polarizare circulară iar în locul vizorului, din partea posterioară a aparatului, se află dispozitivele de afișaj cu diodă luminiscentă rectangulară și un instrument de măsură. În cazul când fascicolul este modulat în amplitudine sau în impulsuri - această situație se semnalizează printr-o altă diodă luminiscentă.

Pentru a feri aparatul de perturbația altor câmpuri electromagnetice de frecvență mai mică, acesta este prevăzut și cu un filtru "trece sus" pentru a elimina semnalele care nu interesează. Banda de frecvență este de la 2 la 12 GHz și eficiența de depistare a microemitterului din încăperea de la 1 la 3 m. În cazul când există fascicule cu care este bombardat, în mod util, elementul pasiv din încăperea, în mod sigur ele vor fi evidențiate deoarece aparatul prezintă o sensibilitate mai bună decât cea necesară elementului pasiv.



MIJLOACE GENERALE DE PROTECȚIE ÎMPOTRIVA TUTUROR TIPURILOR DE INTERCEPTĂRI

Cu toată eficiența și rezultatele pozitive obținute prin mijloace de detectare, concepția privind dezvoltarea mijloacelor de protecție a cunoscut o dezvoltare continuă. Ea își propune nu să depisteze dispozitivele de interceptare, ci, plecând de la premisa că acestea există, caută prin diferite procedee acustice (bruiere electromagnetică, ecranări) să le anuleze sau să le reducă la minim efectele (interceptarea și transportul semnalului util).

De cele mai multe ori, în special în instituții guvernamentale, politice și chiar societăți comerciale care au interese deosebite în apărarea secretului de fabricație, a politicilor de dezvoltare etc. cele două concepții nu se exclud. Astfel, deși periodic se execută controale de depistare, având totuși în vedere costul ridicat al acestora și datorită ușurinței cu care mijloacele de interceptare pot fi reamplasate, se folosesc mijloace de protecție generală împotriva interceptării permanent sau pentru momente importante, sau când se discută probleme deosebite și se iau hotărâri deosebit de secrete.

Camerele acustice din încăperi, botnițele și generatoarele de bruiaj

Dintre procedeele de protecție acustică ce urmăresc ca discuțiile să nu poată fi captate de microfonul dispozitivului de interceptare, cu sau fără fir, vom prezenta și ne vom spune părerea, la început despre cele mai proliferate. Astfel, s-a răspândit și în unele cazuri a devenit obișnuință, ca odată cu începerea unei discuții să se crească volumul audiiiei la aparatul de radio, să se pornească magnetofonul etc. Aceste măsuri care s-au popularizat (neintenționat) de multe ori în filme, nu fac decât

să îngreuneze activitatea celor ce interceptează dar nu pot da o siguranță celor supravegheați.

Este grav faptul că s-a răspândit convingerea conform căreia procedând astfel, vocile nu pot fi înțelese, chiar dacă sunt interceptate. Realitatea este că, prin instalații de interceptare stereofonică (cu două microfoane și două canale de transmitere diferite), prin extragerea semnalului util din zgomotul de fond, sau a "scăderii" electronice a emisiunii radio înregistrate din semnalul captat (pentru că emisiunea radio este aceeași, atât din punctul de interceptare cât și la cel de înregistrare) se poate obține practic numai discuția utilă nealterată. Pentru cei care încă nu sunt convinși că ridicând volumul aparatului de radio nu realizează nimic bun, vrem să le spunem că în aceste condiții, fără să-și dea seama, măresc și ei pragul acustic al discuției, așa că raportul semnal util (discuție) - zgomot (emisie radio) rămâne același.

Rezultate ceva mai bune se obțin când se folosesc surse de zgomot care distribuie energia acustică uniform pe toate frecvențele folosite de vocea umană, ca cele produse de apa care curge prin robinetele deschise, zgomotul ventilatoarelor din cameră etc.

Pentru a obține efecte de protecție mai substanțiale s-au construit și comercializat aparate care produc zgomote albe sau altele ce livrează un zgomot alcătuit dintr-un amestec de voci umane (voci-babel).

Cele mai eficiente, dar care nu sunt la îndemâna oricui, sunt camerele acustice (surde) și așa numitele dispozitive botezate botnițe. Prima a fost inspirată din experiența obținută cu aceste încăperi speciale de către laboratoarele electronice pentru măsurători acustice de mare eficiență, în special asupra microfoanelor când este necesar să nu fie influențate de zgomote și trepidații din exterior. Dacă acestea nu pătrund din exterior către interiorul camerei acustice este clar că nici ceea ce se discută în ea nu poate fi recepționat, captat din afară. Pentru necesitățile de laborator, acestea se construiesc cu pereți dubli, umpluți cu vată de sticlă și în exteriorul camerei se plachează cu un strat subțire de plumb iar pentru evitarea trepidațiilor, pe lângă faptul că acestea se plasează la subsoluri, se montează întreaga cameră pe pufere de cauciuc. Mai simplu executate, din materiale care le avem la dispoziție: lemn, plexiglas sau polistiren expandat sunt fabricate și camerele în camere, cum mai sunt numite aceste

construcții de protejare acustică. Ele au dimensiuni de 3 x 4 x 1,5 m. și se montează pe picioare de cauciuc sau sticlă pentru a putea inspecta, observa permanent și preveni eventualele pătrunderi.

Toate adăugirile constructive care se fac în interiorul acestor camere surde, cu lumină electrică de la rețeaua orașului și nu portabilă de la baterii sau acumulatori, aer condiționat, ventilatoare, îmbunătățesc condițiile de lucru în acestea (care nu sunt cele mai bune) dar în același timp reduc din siguranța oferită păstrării secretului comunicărilor.

Pentru a putea realiza convorbiri absolut sigure împotriva interceptărilor în orice încăpere a unui imobil și nu numai unde este constituită camera acustică s-au fabricat dispozitive portabile asemănătoare ca principii de funcționare instalațiilor de teleconferință, de sonorizare a unor săli de traducere simultană. Aparatul este prevăzut cu 8 - 12 locuri de lucru, fiecare dispunând de o cască în care să se audă tot ce se vorbește și care se mulează bine pe urechea ascultătorului sau care având dimensiuni mici se înfundă în ea. Microfonul este montat într-un dispozitiv care acoperă gura celui care vorbește (de aici și denumirea). Astfel participanții pot conversa, fără ca semnalele să fie captate în jurul lor, în interiorul camerei. Cu tehnologia actuală aparatura poate fi construită de dimensiuni foarte mici și chiar împreună cu anexele ("botnițele" și "căștile") poate fi transportată în 1 - 2 valize diplomat sau o geantă.

Trebuie să arătăm că datorită incomodității și disconfortului ce-l provoacă celor ce sunt obligați să le folosească, aceștia nu le agreează și caută să le evite atât cât le permit regulile de muncă, stabilite de superiorii lor.

*

* *

Unele laboratoare pentru măsurători în domeniul frecvențelor înalte au realizat așa-numitele încăperi blindate sau ecranate care le izolează de toate câmpurile de RF; cei care se ocupă cu protecția împotriva interceptărilor au construit încăperi sau porțiuni ale acestora asemănătoare celor prezentate mai sus. Cu ajutorul blindării cu tablă sau plasă metalică s-a reușit ca

semnalele R.F. ale eventualelor microemițătoare să nu poată străbate încăperile, ori ca fasciculele de microunde să nu poată pătrunde pentru activitatea dispozitivelor pasive.

Protecția oferită de aceste ecranări este cu atât mai mare cu cât este îndreptată împotriva unor câmpuri ce se află în partea de sus a benzilor de frecvență și devin mai puțin utile împotriva semnalelor de frecvență mai joasă.

Numai faptul că se discută, se proiectează și se construiesc camere surde sau ecranate, foarte costisitoare, ne arată că nimic nu-i prea scump pentru protecția secretului. În țările în care nu sunt interzise prin lege, se folosesc dispozitive de bruiaj electronic pentru protecția împotriva interceptărilor cu aparatura de radiofrecvență. Se perturbă astfel receptoarele de interceptare, prin faptul că ele captează și acești paraziti odată cu semnalul util de la microemitătorul ascuns. Efectele negative ale acestor generatoare de bruiaj sunt cunoscute odată cu influențele unei bobine de inducție auto sau ale altui dispozitiv producător de scântei, nedeparazitat asupra calității audiției unui receptor auto.

Tot în categoria generatoarelor de bruiaj le încadrăm și pe cele magnetice care acționează asupra microfoanelor, capetelor de magnetofon, telefoanelor etc. Partea terminală a acestora este fie o bobină centrală de dimensiuni mari, fie un cablu care înconjoară încăperea protejată și care joacă un rol de antenă. Ele sunt alimentate de un amplificator de putere (sute de wați) care amplifică "brumul" ce se va induce în dispozitivele de interceptare. Rezultatele cele mai bune se obțin când amplificatoarele sunt alimentate la intrare de un generator de zgomot alb. Deficiențele acestora constau în puterea prea mare necesară pentru a fi eficiente și de aici faptul că paraziții se induc și în alte aparate electronice (telefon, aparate de recepție) din vecinătate, cu reclamațiile respective. Pentru protejarea împotriva emițătorului cu curenți purtători utilizați pe linie telefonică și pe rețeaua electrică se folosesc cu succes filtre montate în special pe cabluri telefonice. Acestea împiedică trecerea în rețeaua telefonică a semnalelor de frecvență peste gama audio și mai ales în domeniul 20 - 50 KHz în care funcționează acestea. Greutăți apar în construirea filtrelor pentru rețele electrice, deoarece consumurile mari necesită bobine (din componența filtrelor) de dimensiuni foarte mari.

Deși la sfârșitul unui capitol anterior acestuia s-a relatat despre echipele care execută acțiunea de contracarare, de curățire cum mai este denumită acțiunea de localizare și depistare a dispozitivelor de interceptare, montate clandestin, în continuare dorim să arătăm următoarele: în țările dezvoltate, în afara activităților guvernamentale pe care nu le tratăm dar despre care spunem că sunt cele mai profesionale, au luat ființă multe societăți care își oferă serviciile în aceste domenii, folosind o paletă largă de echipament electronic. Cele care solicită prețuri minim, "agită" niște aparate de măsurare a câmpului magnetic, verifică tapițeria sau mobila și desfac capacul telefonului. Dau în schimb, garanții maxime că spațiul controlat este "curat". Sunt însă și firme serioase care își fac treaba conștiincios, solicită în jur de 1000 dolari S.U.A. pe oră de control dar dispun și folosesc cele mai sofisticate aparate, au personal recrutat și format din cei care au acționat în C.I.A., F.B.I., M.I. 5, M.I. 6, Biroul 2 și alte organizații similare. La noi în țară controlul în domeniul privat este la început dar va urma sigur aceeași cale ca în țările dezvoltate, odată cu creșterea rolului asigurării secretului în activitatea politică, economică, de presă și a creșterii concurenței în toate domeniile arătate mai sus.

Si la noi ca și în occident, numai anumite instituții nominalizate aparținând de puterea executivă sau judecătorească pot, în condiții stabilite de lege, să folosească mijloace de interceptare. Asta nu înseamnă însă că în lupta de a cuceri noi piețe, de a afla și ieși înaintea concurentului cu un produs la vânzare, de a apăra sau fura secretul de fabricație, de a afla primii ce s-a discutat la ședința colegiului director al unui partid pentru a relata primii în presă, nu se vor folosi și astfel de procedee de interceptare, cu riscul de rigoare. De altfel în raportul S.R.I. înaintat Parlamentului României în iulie 1993 se arată că se dețin dovezi clare de folosire a acestor metode în țară.

Dacă sunt folosite mijloace ofensive se creează automat și aparatură de contramăsuri și se formează echipe specializate pentru protecția celor care le solicită și au nevoie de ele.

La sfârșitul acestui capitol se consideră util și instructiv pentru cititori să redăm din presa occidentală date recente, referitoare atât la tehnica de interceptare cât și la cea de detectare, a contramăsurilor - relatări, determinate de scandalul provocat de descoperirea unor interceptări folosite de rețeaua "Godo", condusă de Fernando Rodriguez Gonzales, fost colonel al Centrului Superior de Informații al apărării din Spania (C.E.S.I.D.).

Astfel cotidianul spaniol "ABC" din 28 noiembrie 1993 publică articolul "Guvernul tolerează vânzarea liberă a unor sisteme pentru spionajul privat". Din conținutul acestui articol, semnat de Alfredo Semprun, prezentăm următoarele:

"De câțiva ani încoace, majoritatea marilor întreprinderi spaniole au trebuit să introducă pe lista lor de cheltuieli un nou capitol: securitatea. Și, întrucât cu un emițător în miniatură care nu costă mai mult de 30000 de pesetas oricine se poate transforma într-un James Bond, ce se poate întâmpla atunci când se aliază geniile electronicii cu foștii agenți secreți? Astăzi, un spion poate intercepta din Australia o conversație purtată într-un birou din Madrid, cu condiția ca în apropiere să se afle un telefon (n.a.: Puțin cam exagerat!). Inșă dezvoltarea electronicii are o dublă direcție. Aceleași sisteme care se folosesc la furtul unor secrete industriale sau la obținerea unor poziții avantajoase în cadrul unor negocieri comerciale sunt capabile să și protejeze de urechile indiscrete. Totuși, cea mai bună protecție ar constitui-o o lege care să restrângă comercializarea acestor mici minuni tehnice și care să pedepsească folosirea lor ilegală ..."

"În urmă cu numai patru luni, un inginer italian necunoscut a pus în practică un sistem ingenios menit să intercepteze telefoanele celulare ..."

"Invenția costă trei milioane de pesetas și folosește un căutător de frecvență, asistat de calculator, care identifică codul personal al telefonului și îl captează de fiecare dată când cel care îl folosește lansează în eter semnalul de apel. Bineînțeles, întregul echipament este portativ și poate fi completat cu un detector de automobile. Concurența, în acest caz israelienii, a scos pe piață

la începutul lunii octombrie 1993 un sistem similar, însă mult mai sofisticat - poate programa până la 80 de numere ..."

"În Elveția, alt inginer specialist în telecomunicații a reușit să fabrice un < <microfon> > pentru telefon nu mai mare decât un bob de orez și care are în plus aspectul unui nevinovat component electronic. Și (...) la Mataro (Barcelona) un mic atelier, proprietatea unui anume Ignacio, se montează minuscule emițătoare radio, capabile să transforme scrumiera dintr-un birou într-o sucursală a B.B.C..." (n.a.: British Broadcast Corporation, post de radio și televiziune)

"Pe terenul spionajului electronic, tehnica evoluează foarte repede! (...) Oricare cetățean care dorește să știe ce părere au cu adevărat despre el subordonații săi, soția sau vecinul, nu are decât să se apropie de magazinul din Andora al lui Alan Paterson pentru a obține echipamentul corespunzător. În funcție de prețul pe care este dispus să-l plătească poate obține de la un simplu magnetofon care începe să funcționeze de fiecare dată când vorbește cineva și care dispune de o autonomie de șase ore, și până la un emițător complet de televiziune de mărimea unui pachet de țigări. El nu trebuie să ofere explicații. Lipsa unei legislații îl pune la adăpost, cu condiția să nu ofere altor persoane respectivele informații (...). În plus, nici vânzătorii nu pun întrebări..."

"Majoritatea clienților mei - declara Alan Paterson - sunt detectivi privați sau oameni de afaceri care îl suspectează de infidelitate pe vreunul dintre angajații lor. Nu e treaba mea ce fac cumpărătorii cu respectivul material. Paterson fabrică aceste tipuri de aparate, cu toate că cea mai bună invenție a sa are o destinație total opusă: este un detector de frecvență care localizează radioemițătoarele și mai are un sistem pentru descoperirea microfoanelor ascunse, chiar dacă respectivele microfoane nu funcționează în acel moment. Totuși, Paterson s-a hotărât să se lipsească de telefonul din atelierul său din Barcelona, ca măsură ... complementară de securitate ..."

"Telefonul, după ce primește vizita unei echipe profesionale de spioni, se transformă întotdeauna într-un indiscret prin excelență. Însă microfonul poate fi amplasat oriunde. Există cel puțin două duzini de sisteme de interceptare, transmitere și înregistrare a unei conversații. De asemenea, pot fi interceptate sau deturnate faxuri și desigur, datele transmise prin calculator.

Chiar și o conversație în aer liber poate fi captată cu microfoane direcționale de la distanțe mai mari de două sute de metri (...). Ceea ce pare o simplă cameră video de uz personal poate ascunde un teleobiectiv care mărește de 64 de ori. Imaginile obținute tratate prin ordinatator, ar putea constitui probe de acuzare perfect valabile ..."

"Dacă îi exceptăm pe cei ca Paterson, (...) în Spania există doar vreo șapte întreprinderi de securitate capabile să neutralizeze toate aceste posibile amenințări. Însă sunt foarte discrete, aproape mute când este vorba despre metodele lor. Asta fiindcă una e să descoperi un microfon în cutia telefonului și cu totul altceva este să treci prin filtru 15 km de cablu telefonic sau să descoperi un microfon ascuns într-o priză din perete care, în plus, folosește însăși linia electrică a clădirii pentru a transmite vocile ..."

"Un echipament de contraspionaj de calitate costă 30 milioane de pesetas și cântărește peste 70 kg, afirma reprezentantul uneia dintre respectivele firme cu sediul în Barcelona. Pentru a-l manevra este nevoie de specialiști cu mulți ani de experiență la activ și care să știe, de exemplu, să facă distincția între defectele aparținând liniei telefonice și anomaliile pe care le provoacă un microfon. Fără îndoială că toate manipulările străine pot fi descoperite, cu excepția ascultărilor telefonice oficiale, care sunt făcute chiar de centrala telefonică, pe baza autorizației juridice și care sunt, în consecință, absolut imposibil de detectat. Descoperirea celorlalte nu este simplă. Este nevoie de echipe cu specialiști din diferite domenii și de multe ore de muncă ..."

"Nu e simplu. Să ne imaginăm că în biroul șefului programelor unui canal de televiziune, unde se discută viitoarele achiziționări de programe se vorbește despre bani, a intrat o echipă de agenți privați ..."

"Pentru a pătrunde în locul respectiv, au avut nevoie de un complice ori s-au infiltrat în rândurile personalului care face curățenie, metodă mult mai simplă decât aceea de a se deghiza în lucrător la o companie telefonică. Din acest moment, se deschide o gamă vastă de posibilități. Prima ar fi aceea de a instala un radioemitter în sistemul de aer condiționat și de a practica un orificiu de mărimea capului unui ac cu gămălie în plafonul fals, pentru a plasa acolo microfonul fără fir. În stradă, în interiorul unui

automobil, este instalat sistemul de recepție, format dintr-un aparat de radio fixat pe aceeași frecvență și dintr-o baterie de magnetofoane cu opt piste. Microemițătorul intră în funcțiune când cineva începe să vorbească și, desigur, posedă sisteme auxiliare care elimină muzică și alte zgomote de fond (n.a.: foarte interesant!). Este simplu și ieftin, însă prezintă anumite probleme. Prima este necesitatea de a instala receptorul în apropierea clădirii, întrucât acesta are rază scurtă de acțiune. Cea de a doua o reprezintă faptul că autonomia depinde de bateriile aparatului. A treia problemă este posibilitatea de a fi ușor detectat printr-o atentă examinare vizuală sau prin intermediul unui detector care caută prezența oricărui obiect care conține semiconductori..."

"Alte sisteme elimină aceste inconveniente, însă au nevoie de o tehnologie mai sofisticată și, mai ales, de timp pentru instalarea lor. Unul dintre aceste sisteme este așa numitul <<microfon infinit>>, care trebuie plasat în interiorul telefonului și care captează sunetele din jur, respectiv, tot ceea ce se vorbește în încăpere. <<Magia>> constă în raza sa de acțiune de la Madrid și până în Australia (!). Aparatul <<infinity>>, este alimentat prin intermediul rețelei telefonice respective, și astfel nu are nevoie de baterii, el funcționează la un simplu apel. Când sună și este ridicat din furcă începe să transmită și nu se oprește până ce persoana care a făcut apelul (...) nu întrerupe comunicația. Pentru a fi descoperit este nevoie de un analizor telefonic ..."

"Dacă agenții reușesc să pătrundă într-un apartament vecin sau se află în orice alt birou al întreprinderii, respectiv sunt niște funcționari infideli, poate fi folosită o metodă infailibilă: microfonul din priză. Transmițătorul este ascuns în apropierea unei surse de curent (clădirile moderne pentru birouri, care au cablurile dedesubtul podelei false, corespund cât se poate de bine acestui scop) și vocea este transmisă prin cablul electric până la orice altă priză, de unde este efectuată ascultarea. Instalația are un avantaj în plus: nu are nevoie de baterii fiindcă se alimentează de la rețea..."

"Cu toate că recentul caz de spionaj descoperit la Barcelona (n.a.: <<Rețeaua Godo>> - prezentat în anexele lucrării) a pus accentul pe agresiune (tehnică ofensivă), 90 la sută din <<spionii electronici>> care acționează în Spania lucrează în tabăra opusă, respectiv în <<apărare>> (n.a.: detectare, contramăsuri). Pe noi - afirmă un fost inspector de poliție devenit

om de afaceri - ne angajează marile firme atunci când propriile lor sisteme de securitate sunt depășite de tehnologia agresorului sau de infiltrarea unor angajați neloiali, lucru care se întâmplă mai des decât se crede ..."

"Un exemplu tipic l-ar putea constitui un furt la scară mică, însă continuu, în interiorul magazinelor unei întreprinderi comerciale. Când are loc un eveniment de acest gen, sistemele obișnuite de securitate nu sunt de folos deoarece delicventul este, de obicei, un angajat care cunoaște modul de funcționare al acestora și și-au creat o rețea de complici. În aceste cazuri întreprinderile de securitate electronică obișnuiesc să instaleze camere video în miniatură care, având niște obiective de un milimetru și jumătate în diametru, sunt ușor de ascuns. În plus, pentru a nu trezi suspiciuni în rîndul posibililor vinovați, monitorul care primește imaginile este plasat la o distanță de câțiva kilometri. De fapt, este vorba despre un emițător de televiziune în miniatură care este declanșat prin intermediul unui senzor de mișcări, încorporat și care trimite imaginile monitorului prin intermediul undelor. Același sistem poate fi utilizat pentru paza birourilor și a arhivelor în afara orelor de program". (n.a.: Sistemul TV intră în funcțiune numai când se schimbă imaginile din locul supravegheat).

"<<Apărarea>> este folosită și în cazul extorcărilor, ca un mijloc de obținere a probelor. Victima șantajului va veni la locul stabilit având asupra sa un microtransmițător ascuns. Însă dacă se dorește evitarea riscului ca șantajistul să aibă în buzunar un minidetector de microemițătoare, vor trebui instalate emițătoare miniaturale de mare putere, care să înregistreze de la distanță întreg scenariul întâlnirii ..."

"Până ce nu va fi perfecționat un sistem de ascultare care să permită captarea convorbirilor eliminându-se necesitatea apropierii fizice de obiectiv, spionajul poate fi contracarat sau limitat fie și numai de durata de funcționare a mini-bateriei unui emițător autonom ascuns ..."

"<<Apărarea>> nu este scumpă. O întreprindere serioasă (*de control și detectare a tehnicii de interceptare*) care nu promite detectarea intervențiilor cu acoperire juridică (cele făcute de instituții abilitate) întrucât acest fapt este imposibil, încasează 300000 de pesetas pentru o analiză de securitate care include controlul liniei telefonice și a unei centrale de până la 12 posturi,

o analiză a spațiului în două apartamente - cu detectarea microfoanelor <<adormite>> - precum și controlarea faxului și a computerului ..."

"Poate că totuși, cea mai bună apărare ar consta într-o legislație care să-i descurajeze pe spioni. În S.U.A., după <<Watergate>>, au fost închise 200 de întreprinderi care comercializau produse de acest tip. Delictul nu a putut fi eradicat, însă au fost pedepsite organizațiile care se ocupau cu extorcarea și cu spionajul comercial. În Europa, atât fabricarea cât și vânzarea aparaturii electronice este liberă și folosirea neautorizată nu este pedepsită decât cu cel mult un an de închisoare, în cazul în care nu este asociată altor delikte (...)"

În același articol este publicat "Portretul unui agent". (n.a.: pentru executarea contramăsurilor) Redăm integral cele publicate:

- A fost un polițist sau membru al Gărzii civile ori a lucrat acoperit pentru serviciile de informații ale statului.

- Trecerea sa în viața civilă s-a produs în urma ofertei făcute de un fost coleg care lucra în cadrul unei întreprinderi private de securitate.

- Cunoaște superficial tehnicile de spionaj electronic și de aceea angajează, la rândul său, pentru lucrările mai dificile, specialiști care acționează în temeiul unui contract pe bază de comandă.

- Principala sa activitate este aceea de contrainformații, de schițare și de executare a unor planuri de securitate integrală pentru marile întreprinderi sau pentru protecția persoanelor particulare.

- Când acționează în calitate de <<franctiror>>, de obicei după ce a părăsit întreprinderea fiind concediat sau din cauză că nu dispune de capacitatea de a se adapta la noua funcție, se stabilește pe post de "detectiv privat" și își folosește vechile relații de pe vremea când lucra în cadrul forțelor de Securitate ale statului.

- Are o oarecare tendință de a păstra informațiile obținute pe parcursul anilor de muncă.

PERSPECTIVELE TEHNICILOR DE INTERCEPTARE, DE SUPRAVEGHERE PRECUM ȘI A METODELOR DE NEUTRALIZARE

În general sunt greu de făcut prognoze exacte și concrete în aceste domenii, dar se poate afirma cu certitudine că aceste tehnici trebuie, în primul rând, să țină pasul și să se poată adapta la progresele realizate în sfera de activități cu care acestea vin în contact. Astfel, în industria de telecomunicații au fost obținute noi realizări iar altele sunt așteptate în viitorul apropiat. Interceptarea, cifrarea sau protejarea acestora trebuie să poată face față acestor progrese, să rezolve problemele complexe cu care se confruntă. Apar multe probleme când trebuie să interceptăm convorbiri telefonice ce se transmit pe cablu cu fire metalice, dar sunt alte greutăți, mult mai mari, când se folosesc fibre optice. Nu-i ușor să interceptezi un fascicol de microunde, între două relee, dar este infinit mai greu când trebuie să detectezi ghiduri de undă îngropată. Sunt probleme complexe dar, cu toate acestea, judecând după rezultatele prezentate și după ingeniozitatea tehnică a celor ce interceptează, se poate aprecia că sistemele de comunicații nu vor rămâne invulnerabile la viitoarea tehnică, din ce în ce mai perfecționată, a ascultărilor clandestine.

În al doilea rând, ca în multe alte domenii științifice și tehnologia acestora trebuie să țină seama de perfecționarea din industria electronică, în special cea a fabricării componentelor electronice. Aparatura de interceptare, de ascultare, de transmitere de informații, de observare, de detectare a beneficiat de toate descoperirile din domeniu începând cu apariția tranzistoarelor (după 1949), a circuitelor integrate, a cipurilor, a cristalelor lichide, a circuitelor de memorare, a microprocesoarelor etc, și nu este nici un motiv ca în viitor să se întâmple altfel.

Nu în ultimul rând, progresul este dat de lupta permanentă care există între mijloacele ofensive și cele defensive.

Se așteaptă progrese importante în aceste domenii și prin

aplicarea cercetărilor din alte sfere de activitate similare ca cea din industria armamentului, a tehnicii de luptă de observare și ochire, cum s-a întâmplat și până acum, în mod deosebit pentru aparatura de supraveghere pe timpul nopții.

Pentru aparatura de interceptare ce se plasează în mod camuflat (emițătoare, amplificatoare, receptoare) și care este alimentată la baterie, se va urmări în continuare reducerea dimensiunilor. Pentru aceasta se va căuta în primul rând micșorarea consumurilor prin noi tehnici de prelucrare a semnalelor, folosind viitoarele microprocesoare cu care se vor echipa noile calculatoare de buzunar. Rezultate spectaculoase trebuie așteptate de la revoluția în domeniul bateriilor electrice, ale căror tehnologii de fabricație au rămas mult în urmă, volumul lor determinând în cele din urmă dimensiunile aparaturii electronice. Se apreciază că vor apare atât baterii nucleare care vor livra microwați pe durata de câțiva ani cât și baterii solare perfecționate.

În domeniul audio, pe lângă aparatura de interceptare și de contramăsuri (microfoane, preamplificatoare, magnetofone) se pare că viitorul va aduce perfecționări notabile. Astfel, sunt necesare idei noi, teoretice și practice, pentru înlăturarea zgomotelor, pentru o nouă tehnică eficientă de prelucrare a semnalelor audio, de găsim de noi posibilități pentru interceptarea discuțiilor purtate în locuri deschise (parcuri, străzi etc.).

Modernizarea noilor magnetofone se va baza cu precădere pe tehnica de imprimare cu microcomputere ce vor condensa semnalul vocal pentru a înmagazina o cantitate mai mare de informații pe o bandă magnetică de o lungime dată. Trebuie perfecționată schema mecanică pentru a permite reducerea dimensiunilor și un control mai precis al mecanismului de antrenare a benzii, care va deveni mai îngustă, mai subțire și mai rezistentă. Se speră ca acest magnetofon să fie mai mic decât un pachet de țigări, chiar sub dimensiunile unei brichete, putând funcționa câteva ore sau chiar zile cu dispozitive de pornire (acustomat) și să poată, având dimensiuni reduse, să înlocuiască emițătorul de corp.

Majoritatea dispozitivelor de interceptare au nevoie de imprimarea, stocarea și memorarea informațiilor. Pe lângă perfecționările ce se vor aduce actualelor magnetofone la care nu se va renunța, pentru anumite aplicații se întrevăd noi tehnologii

care fac apel la memorii realizate cu transfer de sarcină sau cu bule magnetice care vor permite, în volume foarte mici, obținerea de memorii de 10^{12} biți. Când se vor pune la punct toate detaliile de fabricație, memoriile cu semiconductori vor înlocui treptat majoritatea sistemelor de menținere analogice. Bazându-se pe un continuu progres în tehnologia memorărilor cu semiconductori, modulațiile de prelucrare a semnalului și de transmitere de tip "acțiune rapidă" vor cunoaște o extindere și mai largă ca urmare a creșterii vitezei și flexibilității de înregistrare cu semiconductori.

Aceste dispozitive pot înregistra informații optice, video sau de radiofrecvență pe o anumită durată de timp, pentru ca apoi să transmită, sub formă de acțiune rapidă, pachetul complet de date stocate.

Sistemul de captare a vocilor prin microfoane se va perfecționa în viitor, astfel că, pe lângă o reducere a zgomotelor, o filtrare și o direcționare mai bună, să permită identificarea automată a vorbitorului, folosind sisteme de microprocesori și de amprentă vocală. În aceste sisteme ale viitorului se vor introduce prin microprocesoare câteva caracteristici cheie, așa cum sunt identificatorii individuali de voce, iar sistemul va putea selecta, capta și, eventual, transmite informațiile audio prin recunoașterea eșantioanelor de vorbire ale persoanelor ce interesează.

Identificarea persoanelor după voce depășește ca importanță domeniul interceptărilor și ea va avea aplicații deosebite în multe alte discipline, în special în criminalistică. Filmul american "Primul cerc" după celebrul roman al scriitorului sovietic dizident, Soljenițin, a reușit să ne formeze o imagine a cercetărilor și importanței depistării persoanelor după caracteristica vocii.

Dispozitivele cu "microunde" cu reflectoare pasive vor deveni mai interesante și pe măsură ce frecvențele devin mai înalte, ele vor fi tot mai mici, pentru a ajunge în final la numai câțiva centimetri lungime.

În domeniul folosirii laserilor, probabil, datorită aplicării rezultatelor cercetărilor făcute până în prezent și care poate vor mai avea loc în derularea programului "Războiul Stelelor", precum și tehnicii îmbunătățite de prelucrare și înlăturare a zgomotelor, acestora li se vor reduce dimensiunile, prețul de cost, consumul de energie și se va putea trece de la stadiul de laborator la aplicații practice și rezultate concrete, spectaculoase în interceptări.

Cele mai mari greutăți sunt cele organizatorice care conduc la mari cheltuieli umane și materiale. Aici se simte nevoia unei soluții pentru "ascultarea" materialelor înregistrate fără intervenția omului și transcrierea acestora cu ajutorul limbajului direct dintre banda înregistrată (voce) și mașină (ordinador) terminalul respectiv pe care să apară scris materialul interceptat.

Ca urmare a progreselor în miniaturizarea dispozitivelor de supraveghere și urmărire, acestea vor putea fi implantate pe cale chirurgicală și folosite în cazuri de urmărire, liber consimțită. Pentru asigurarea alimentării acestora se va putea în viitor recurge la folosirea energiei biochimice sau biotermice degajate de corpul uman.

Spectaculoase perfecționări, așteptate de la tehnologia viitorului, vor trebui să apară în domeniul contramăsurilor pentru că în acest sector activitatea, cu toate rezultatele obținute datorate detectorului de joncțiuni cu semiconductori se întâmpină greutăți foarte mari pentru detectarea microfoanelor din încăperi sau pentru a avea siguranța că în urma controlului n-au mai rămas dispozitive de interceptare. Tendințele și căile în care se acționează pentru atingerea acestor obiective sunt încă ținute secrete de companiile care fac cercetări în domeniul respectiv, la cererea unor instituții guvernamentale. Echipele ce asigură servicii de contramăsuri în afara celor guvernamentale care sunt bine puse la punct, vor trebui să-și îmbunătățească activitatea atât printr-o dotare modernă, cu o pregătire corespunzătoare a personalului, cât și prin creșterea credibilității rezultatelor activității pe care o desfășoară ca și a garanțiilor pe care le acordă clienților. Se vor stabili, pentru societățile particulare prestatoare de servicii, proceduri și norme de autorizare și standarde pentru evaluarea serviciilor prestate.

În domeniul depistărilor se așteaptă perfecționări spectaculoase ale receptoarelor - goniometre. Astfel, pentru a micșora timpul de exploatare a benzilor de unde scurte în care au loc aceste transmisii rapide, receptoarele pentru detectare se construiesc într-o instalație complexă, formată din 40 - 50 instalații de recepție de bandă mai îngustă, astfel ca baleierea domeniului de frecvență aflat în responsabilitatea fiecărui receptor, deci și a întregii benzi, de către toate receptoarele ce acționează simultan să fie făcută în timp de milisecunde. Se stabilesc criterii speciale asupra caracteristicilor de transmitere ce

interesează (viteza de transmitere, mod de cifrare etc.) pentru a fi eliminate automat semnalele clasice ce nu interesează a fi recepționate.

Cele mai mari greutatea se întrevăd în rezolvarea problemei recepției radioemitoarelor ce funcționează în salturi de frecvență.

Modernizările în aparatura de recepție și goniometrie vor apare în centrele noi de goniometrie și recepție care sunt în construcție în statele puternic dezvoltate. Astfel, în Germania, după cum arată cunoscutul săptămânal german "Der Spiegel" din 26 aprilie 1993, într-un articol nesemnat și intitulat "Totul la ureche" se arată că pentru a nu rămâne mai prejos față de centrele de acest gen ce aparțin de C.I.A. sau de serviciile de informații engleze, Bundeswehr-ul și B.N.D. (serviciul federal de informații german), neimpresionate de sfârșitul războiului rece și de penuria financiară de la Bonn sunt pe cale de a termina construcția unei noi stații de ascultare în landul Schleswig Holstein, care va costa în final 200 milioane de mărci, destinat interceptării și localizării emisiunilor de unde scurte și de înaltă frecvență.

Stația de ascultare ultrasecretă ce va purta numele conspirativ Castagnete, de o înaltă tehnicitate, va fi dată în funcțiune la sfârșitul anului 1995 și se va întinde pe o suprafață (inclusiv antenele) de 100 ha. Se pare că această va fi prima dintr-un lung șir de stații care vor "asculta" tot ce se emite, de la flancul de nord până la granița irakiană. Tot în acest articol se afirmă cu mândrie că va fi posibilă ascultarea pe unde scurte a oricărui dușman potențial de pe glob și a oricăror tipuri de transmisii atât radiofonice cât și telegrafice, telefaxuri, ba chiar se va putea stabili poziția soldaților germani în cazul acțiunilor de intervenție O.N.U..

Pentru serviciul federal de informații B.N.D., această stație de interceptare va fi manipulată, prin computere, din sediul acestuia de la Pullach.

Sunt numai câteva direcții în care se va acționa pentru perfecționarea în viitor, având în vedere înlăturarea unor greutatea cu care se mai confruntă interceptarea și în mod deosebit depistarea și protecția.

A N E X A I

UTILIZAREA SPECTRULUI DE FRECVENȚĂ ÎN S.U.A. ȘI ÎN UNELE ȚĂRI OCCIDENTALE

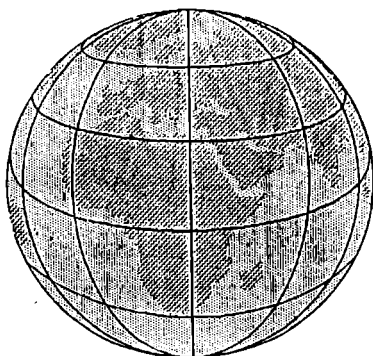
SPECTRU DE FRECVENȚĂ

0 Hz ÷ 16 Hz	- infrasunete
300 Hz ÷ 16 KHz	- sunete
16 KHz ÷ 60 KHz	- ultrasunete

SPECTRU RADIOFRECVENȚĂ

1 KHz ÷ 10 KHz	- Frecvență extrem de joasă
10 KHz ÷ 100 KHz	- Alocare internațională
100 KHz ÷ 500 KHz	- Foarte joasă frecvență
500 KHz ÷ 1600 KHz	- Unde medii - Radiodifuziune - modulație de amplitudine
1600 KHz ÷ 1800 KHz	- Alocată pentru marină
1800 KHz ÷ 25 MHz	- Unde scurte - alocare internațională - Radiodifuziune etc.
25 MHz ÷ 30 MHz	- Alocare publică - (Citizen band)

30 MHz ÷ 50 MHz	- Pentru servicii guvernamentale și publice
50 MHz ÷ 72 MHz	- Televiziune canal 2 - 4
73 MHz ÷ 88 MHz	- Televiziune canal 5 - 6
88 MHz ÷ 118 MHz	- Radiodifuziune FM
118 MHz ÷ 135 MHz	- Alocată Aviației pentru Comunicații în fonie
135 MHz ÷ 174 MHz	- Alocată poliției și problemelor de industrie și afaceri
174 MHz ÷ 920 MHz	- Televiziune Canale 7 - 11; 14 - 83
920 MHz ÷ 5,5 GHz	- Microunde
5,6 GHz ÷ 10 GHz	- Comunicații sateliți
10 GHz ÷ 1000 GHz	- Unde milimetrice, submilimetrice
> 1000 GHz	- Infraroșii, lumină vizibilă ultraviolet (laseri) - raze X, raze gama



A N E X A II

BENZILE DE FRECVENȚĂ ȘI DENUMIRILE LOR

Banda de frecvență	Lungimea de undă	Denumirea metrică (unde)	Prescurtarea denumirii metrice	Simboluri în limba engleză	Alte simboluri și denumiri
3 + 30KHz	100km + 10km	miriametrice	B.Mam	VLF	unde foarte lungi FJF și ULF
30 + 300KHz	10km + 1km	kilometrice	B.Km.	LF	unde lungi JF, UL
300 + 3000KHz	10hm + 1hm	hectometrice	B.hm.	MF	unde medii UM
3 + 30MHz	10dam + 1dam	decametrice	B.dam.	HF	unde scurte IF, US
30 + 300MHz	10m + 1m	metrice	B.m.	VHF	unde foarte scurte FJF, VFS
300 + 3000MHz	10dm + 1dm	decimetrice	B.dm	UHF	unde ultrascurte VIF, VUS
3 + 30GHz	10cm + 1cm	centimetrice	B.cm.	SHF	unde suprascurte SIF, VSS
30 + 300GHz	10mm + 1mm	milimetrice	B.mm	EHF	unde extrem de scurte EJF, UES
300 + 3000GHz	1mm + 0,1mm	submilimetrice	-	-	-

A N E X A III

APARATURA DE INTERCEPTARE ROMÂNEASCĂ DUPĂ DECEMBRIE 1989

Dacă a m putea da timpul înapoi și ne-am afla în acele zile fierbinți din Decembrie 1989 și în primele luni ale anului următor, multe lucruri nu le-am rezolva acum, așa cum le-am făcut atunci.

Ca să fim corecți, trebuie să spunem că date fiind condițiile concrete de atunci, poate unele nici nu se puteau rezolva altfel.

Nu ne propunem să ne referim aici la toate aceste aspecte și ne rezumăm numai la unul care la prima vedere poate părea minor sau chiar deplasat față de multe alte probleme grave ce au fost soluționate necorespunzător. Abordarea problemei respective a fost provocată și de campania dezlănțuită pentru a întreține o psihoză anti-interceptare, anti-servicii speciale de informații. Din fericire acum toată această zarvă începe să se estompeze.

După revoluție, în loc să condamnăm, așa cum era normal, folosirea abuzivă a mijloacelor tehnice de interceptare a convorbirilor unor persoane, care nu aveau altă vină decât aceea de a nu fi fost de acord cu ideile unui singur partid, cu cultul deșănțat al personalității, cu cenzurarea literaturii și câte multe altele, noi am distrus și toate mijloacele tehnice de interceptare, canalizându-ne ura împotriva unor instalații, cable, amplificatoare, magnetofone și altă aparatură specifică. Am dezafectat clădiri, am tăiat cabluri telefonice, am casat aparatură, am aruncat la gunoi miliarde de lei. Nu era mai bine ca aceste instalații să fie conservate și apoi predate fie poliției pentru a o ajuta în descoperirea infractorilor din multele dosare cu autori necunoscuți, în lupta împotriva corupției și a mafiei românești, fie gărzii financiare, ca mijloc complementar în lupta împotriva evaziunii fiscale, fie procuraturii în anchetarea cauzelor date în competența ei, în special pentru identificarea autorilor de crimă, fie vamei, fie - și nu în ultimul rând - serviciilor de informații interne și externe, cărora le revin obligații deosebite în apărarea

siguranței statului indiferent ce guvern sau partid ar conduce țara la un moment dat?

Suntem de acord cu toții ca în țară să fie prinși cât mai repede criminalii, să fie stârpită complet corupția, să fie sancționați toți cei care comit evaziuni fiscale, să nu aibă loc acte teroriste, să nu se introducă și să nu se vândă droguri, să nu avem tentative sau atacuri împotriva siguranței statului, a ordinii de drept, iar acestea, dacă se produc, să fie depistate la timp. Imi vin în memorie unele întrebări și interpelări făcute cu diferite prilejuri: Ce a știut S.R.I.-ul în această problemă? Ce informații a avut și cui i le-a trimis? Ce face poliția împotriva corupției? Cum au putut să pătrundă toate aceste obiecte în țară? Ce face vama? ș.a.m.d.

Cetățeanul, pe bună dreptate, dorește să fie apărat de către instituțiile de stat, să se simtă în siguranță dar, din păcate, el nu poate realiza cum se poate îndeplini un asemenea deziderat. Sunt convins că s-a reținut faptul că în toate interviurile și declarațiile reprezentanții acestor instituții au arătat că n-au o dotare suficientă. Sigur, prin acestea, mulți au înțeles că e vorba despre autoturisme și mijloace de transmisiuni dar și de aparatură tehnică pentru obținerea și verificarea informațiilor pentru aflarea adevărului, deși aceștia, din păcate, n-au spus-o clar.

Rezolvarea deplină a acestei probleme nu este simplă. Opinia publică încă asociază aceste mijloace de tehnică operativă cu totalitarismul, cu securitatea și comunismul. Nu realizează ce dimensiuni au luat astăzi criminalitatea, acțiunea de trădare - spionaj, de evaziune fiscală, corupția etc. Oare nu vrem să constatăm cât suntem de 'cercetați' de serviciile de informații ale unor țări atât din Vest cât și din Est, dat fiind poziția noastră geopolitică în această zonă agitată în lume?

Trebuie să se înțeleagă că aceste mijloace și instituțiile care le folosesc nu sunt ale puterii actuale ci în primul rând - sunt ale țării, că peste o anumită perioadă mai scurtă sau mai lungă de timp, alții pot fi la putere și că, de frica unor abuzuri care se pot întâmpla oricând și oriunde nu avem voie să nu beneficiem de mijloacele puse la dispoziție de știința și tehnologia modernă.

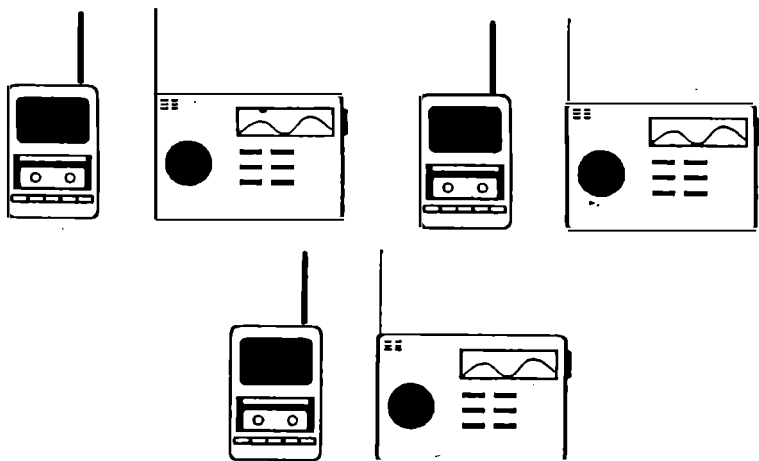
Nu vreau să se înțeleagă că la noi în țară este un vid juridic sau că nu există nici un fel de reglementări corespunzătoare în materie. Legea privind siguranța națională, în special prin art.13, a dat o anumită rezolvare problemei, în sensul că stabilește în ce

scop pot fi folosite interceptările, care sunt instituțiile ce pot apela la aceste mijloace, cine aprobă, precum și sancționarea abuzurilor din acest domeniu.

Din păcate, până la aplicarea completă mai este cale lungă de străbătut. În afara unei timidități manifestate de instituțiile în drept, explicabilă fiecărui început, trebuie stabilit, fie printr-o lege specială, fie prin alte acte normative, cine este abilitat să administreze aceste interceptări (cred că ar fi prea scump ca toate instituțiile să-și construiască centre de interceptare), ce obligații revin în mod deosebit Ministerului Telecomunicațiilor și toate detaliile de cooperare cu instituțiile abilitate prin lege.

Să nu uităm că în primul rând trebuie să reconstruim, din păcate; mijloacele tehnice pe care le-am dezafectat și fără de care instituțiile respective nu pot beneficia de prevederile legii.

În alte articole precum și în extenso în această lucrare s-au prezentat date privind modul cum este rezolvată această problemă în multe alte țări dezvoltate. Sper că nu vom fi acuzați că am încercat să denigrăm prin aceasta Occidentul, capitalismul - noi dorim doar să demonstrăm că problema interceptării comunicațiilor nu este o invenție și practică românească.



**"ZIARIȘTII ȘI SURSELE LOR"
ABORDEAZĂ PROBLEMA
TEHNICII DE INTERCEPTARE**

Febra interceptării telefoanelor a cuprins în cele din urmă și "Tinerama" care în numărul 116 din 19 februarie 1993 într-un articol pe două pagini, realizat de domnul Ioan Itu, prezintă după o documentare 'riguroasă' destul de 'anevoioasă', așa cum singur afirmă, modul de reglementare și folosire a interceptării convorbirilor în diferite țări europene, inclusiv la noi.

Nu știu de ce autorul face atâta caz de o așa zisă activitate laborioasă de documentare și de ce nu ne prezintă sursele de informare. Nu este profesional și corect să p. .zinți care este situația în Franța, fără să spui că te-ai inspirat din articolul "Les Oreilles de l'état" din "Science et Vie" - iunie 1992. Problema respectivă a fost tratată înaintea "Tineramei", de multe alte cotidiane și săptămânale, în special "Libertatea", care începând din 16 februarie 1993, a prezentat în serial traducerea integrală a articolului din revista franceză, dar a nominalizat sursa de documentare cum este cinstit să facă toți publiciștii. Aici nu poate fi vorba de dreptul unui ziarist de a-și acoperi sursele de informare pentru că în cazul de față acesteă sunt publice ci mai degrabă de eludare sau încălcarea dreptului intelectual a copyright-ului.

Dar să lăsăm sursele externe pe care le-a folosit fără ca autorul să le nominalizeze și să acordăm spațiul ce i se cuvine documentării privind situația trecută și prezentă a interceptărilor din țara noastră. Nici pe aceste surse autorul nu le face cunoscute. Înainte de a i le prezenta noi, dorim să-i atragem atenția că necitându-le își asumă întreaga răspundere a afirmațiilor pe care le-a făcut. De aceea, pentru toate neadăvrurile (ca să nu le spunem minciuni) debitate în articolul din "Tinerama", îl considerăm principal vinovat pe domnul Ioan Itu și apoi pe I.M.Pacepa, autorul cărții "Orizonturi roșii" editată în limba română în anul 1988, la New-York, care a constituit principala sursă de

documentare. Îl rugăm pe autor să nu încerce să ne combată și să nege că s-a inspirat din ea, pentru că până și titlul articolului l-a luat din cartea lui I.M.Pacepa.

Acesta, în capitolul al VIII-lea pune titlul "Puterea cu ajutorul microfoanelor" și Ioan Itu în "Tinerama", scrie "Puterea și microfonul". Dacă mai dorește alte argumente pentru a-i demonstra că avem dreptate arătăm că în lucrarea lui I.M.Pacepa se strecoară greșit prenumele unui personaj pe care în realitatea îl cheamă altfel. Ne poate explica autorul articolului din "Tinerama" de ce după "asidua documentare" în "Tinerama" a apărut aceeași greșeală ca cea din lucrarea lui I.M.Pacepa?

Domnul Ioan Itu afirmă (la fel ca I.M.Pacepa) că în anul 1978 s-a prezentat cuplului Ceaușescu un aparat telefonic modificat, prototip, ca pe o realizare tehnică deosebită, premieră mondială, cu ajutorul căruia puteau fi ascultate discuțiile dintr-o încăpăre în care se afla telefonul, chiar dacă microreceptorul acestuia este pe furcă. Dacă ar fi făcut o sumară documentare, citind ceea ce a apărut în presa noastră postrevoluționară ar fi văzut că "fantastica" și "recenta" descoperire prezentată în mai 1978 era rezolvată de 30 de ani. Cel puțin așa rezultă și nu avem motive să nu dăm crezare și din publicarea unor materiale de arhivă de către revista "Magazin Istoric" în iunie 1991, sub semnătura domnului Cristian Popișteanu. În aceste arhive se găsește declarația col. ing. Golumbovici, din conducerea tehnico-operativă a Ministerului de Interne care, anchetat în 27 octombrie 1967, pentru elucidarea asasinării lui Lucrețiu Păstrășcanu arăta că Ministerul de Interne, datorită unei invenții a tehnicianului telefonist A. Smelas, folosea încă din 1948 ascultarea convorbirilor din încăperile unde se afla un telefon modificat.

Rugăm pe domnul Itu să ne aducă pentru a ne convinge o singură dovadă în afara afirmațiilor lui I.M.Pacepa, că s-a organizat o expoziție în 1978 la Brănești, la care au participat soții Ceaușescu și I.M.Pacepa și unde s-a ordonat să se fabrice și să se folosească numai acest telefon, cu care se pot capta convorbirile din jurul lui. În același timp, însă, îl sfătuim să nu piardă timpul, pentru simplul motiv că soții Ceaușescu nu au fost niciodată în acea clădire de la Brănești, că Elenei Ceaușescu nu i s-a arătat atunci și nici altădată vreun aparat construit de institutul la care Ioan Itu face referiri, că Nicolae Ceaușescu n-a dat nici un ordin, iar domnul I.M.Pacepa, sursa de informații a ziaristului, a însoțit

cuplul Ceaușescu la expoziția la care vă referiți numai în visurile lui.

Nu și-a dat seama domnul Itu, că tot ce a scris I.M.Pacepa, în capitolul al VIII-lea, ca de altfel în toată cartea, este rodul unei fantezii bolnăvicioase, că totul nu este decât o minciună? Cum putea fi ascultat un popor întreg pentru care era nevoie de un altul care să facă înregistrarea și redarea discuțiilor? I.M.Pacepa vorbea de ascultarea a 10 milioane de oameni, simultan, începând cu 1984. Ioan Itu, ca să pără mai credibil arată că din informațiile pe care le deține, fabrica Electromagnetica a construit în perioada 1978-1989, în baza ordinului lui Nicolae Ceaușescu 1,5 milioane de telefoane cu amplificatoare, microfoane și diodă (!) incorporate. Vă dați seama ce spuneți domnule Itu? Cum se pot afirma asemenea enormități? Din cele 1,5 milioane de telefoane fabricate în aceste condiții de Electromagnetica, rugăm să se prezinte măcar unul. Dacă, într-adevăr, s-au fabricat atâtea telefoane într-o perioadă de peste 10 ani, trebuie să se găsească un director, inginer sau muncitor de la întreprindere, care să vă susțină afirmațiile. Fabricarea unei cantități așa de mari nu se poate să nu lase o documentație tehnică, după care acestea s-au executat. Publicați-le! Apreciați cât ar fi costat fabricarea a 1,5 milioane de amplificatoare, microfoane și plasarea lor în telefoane? Cine a suportat aceste cheltuieli? Cred că știți că aceste aparate erau recepționate, achitate, montate la abonați și întreținute de M.T.Tc. Credeți că nici un lucrător din întregul corp tehnic al acestei instituții nu și-ar fi dat seama că telefonul are părți componente foarte importante și costisitoare care nu sunt necesare pentru funcționarea normală a acestuia?

Nu se poate asigura secretul unei asemenea acțiuni la care timp de peste 10 ani au participat zeci de mii de persoane. Se pare însă, că pe lângă documentarea principală, deoarece I.M.Pacepa a părăsit țara în 1978, autorul articolului a mai obținut informații pentru perioada 1978-1993 de la persoane neavizate, necunoscătoare, care încurcă datele și îl dezinformează pe autor. Este adevărat că la Electromagnetica prin anii 1960 s-au construit 25 de racuri a câte 40 de magnetofone de înregistrare, după un model al Ministerului de Interne, dar de la magnetofone la telefoane cu amplificator, de la cantitatea de 1000 (40 x 25) la 1,5 milioane precum și la plasarea lor în timp cu diferență de

aproape 20 de ani, este o cale lungă. Cred că domnul Ioan Ițu apreciază cel puțin acum cât de dăunător și periculos este să folosească surse mincinoase. Autorul dorește să intre și în probleme de amănunt, dând detalii privind montarea unui telefon când se dorește interceptarea convorbirilor. Din explicații nu se înțelege un singur lucru, dar de fond și îl rugăm pe domnul Ițu să ne lămurească. Astfel, dacă telefonul tot are încorporat în el un amplificator și dioda (!) de ce lipitura tip "punte" este necesar să se facă de un "depanator" în casa obiectivului urmărit și nu se face din fabricație, ca să fie de la început în circuit amplificatorul. Și de data aceasta domnule Ițu sursa de informații v-a prezentat date greșite, care nu rezistă la cea mai sumară analiză.

Ca să faceți articolul mai atrăgător și revista mai vandabilă s-a publicat și fotografia unei clădiri, dar pentru cititori nu este o noutate, pentru că despre aceasta s-a mai scris foarte mult în presa post-revoluționară. Imobilul respectiv, după cum afirmați și știe toată lumea, aparține astăzi Armatei. S-a prezentat totuși această clădire deși nu aduceți nici o noutate pentru a vă crea posibilitatea să afirmați că din aceasta n-a fost scoasă aparatura de interceptare. Chiar nu credeți că puteți fi invitat de reprezentanții Armatei să vedeți că nu există nici un fel de aparatură în funcțiune, sau conservare și să fiți obligat astfel să cereți scuze?!

Oare în presa noastră se poate scrie orice, fără ca nimeni să răspundă pentru aceasta? Dumneavoastră căutați să răstălmăciți afirmațiile domnului Virgil Măgureanu. Vreți să faceți pe cititori să creadă că Armata se ocupă astăzi cu interceptările. De ce să nu dăm această interpretare, când dumneavoastră, plecând de la afirmația domnului V.M. că nu Serviciul Român de Informații ci alții în țară fac interceptări, publicați fotografia unei clădiri în care până-n 1989 Securitatea organiza interceptările telefonice lăsând să se înțeleagă că aceasta este astăzi a Armatei, în ea găsindu-se vechea aparatură a securității. Mai poate fi dată o altă interpretare conexiunilor pe care dumneavoastră le faceți în articolul dumneavoastră?

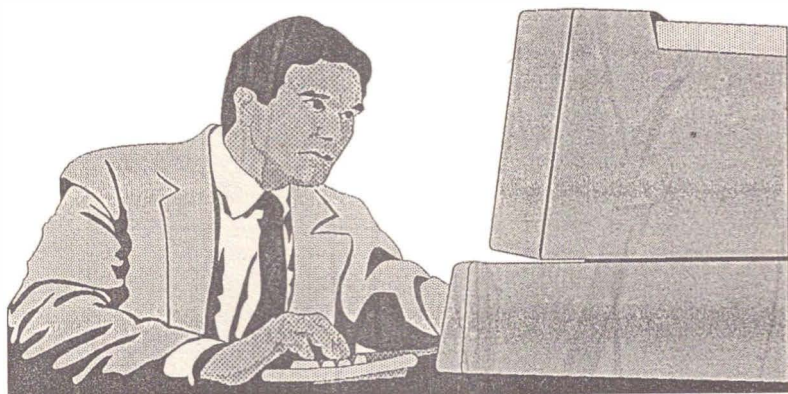
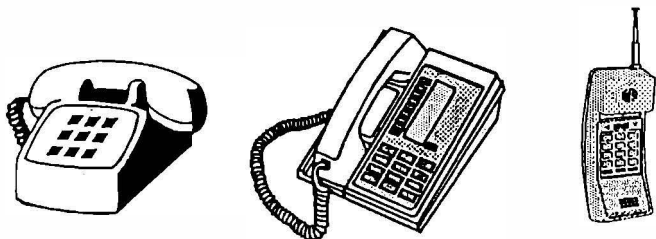
De ce nu vreți să credeți că domnul V.Măgureanu se referea poate la faptul că, sunt ziariști care interceptează discuțiile de la ședințele partidelor pentru a fi primii care să publice anumite știri, că există societăți comerciale care își ascultă concurenții și de ce nu, servicii de spionaj (Est-Vest) care doresc să asculte în

locurile ce-i interesează.

Folosind sursele sale autorul articolului din "Tinerama" a căutat să demonstreze că până în 1989 s-a ascultat un popor întreg și că astăzi practica se continuă și de alte instituții (Armată).

Este o prostie să afirmi că nu s-au făcut în trecut interceptări chiar și în scopuri politice cum îți place să le numească autorul articolului, dar este o aberație să spui că s-a ascultat un popor întreg.

Revizuiți-vă sursele de informații domnule Itu.



UN SCANDAL REFERITOR LA INTERCEPTAREA CONVORBIRILOR ÎN SPANIA

Cotidianul spaniol "El pais" din 16 noiembrie 1993, publică articolul "*A fost distrusă o rețea care asculta convorbirile telefonice ale oamenilor de afaceri*". Din conținutul acestui articol, semnat de Francisco Mercado, redăm următoarele:

"(...) Șapte persoane au fost arestate ieri în capitala catalană, unde au fost percheziționate biroul și domiciliul președintelui ziarului catalan 'La vanguardia', în căutarea de probe pentru spionajul industrial (...). Au fost percheziționate domiciliile din Barcelona ale altor șase arestați. Unul dintre ei, Manuel Maria Sanchez, avea asupra sa, în momentul arestării, aparatură pentru efectuarea de ascultări. De asemenea, au fost confiscate arme reale și simulate".

"(...) Poliția a descoperit cel puțin patru întreprinderi care acționau în Catalonia și care dispuneau de capacități tehnice pentru a executa astfel de ascultări și care obișnuiau să-și ofere serviciile sub acoperirea legală, pentru a realiza asistență în materie de securitate electronică și de întreținere a rețelei telefonice și realizarea de rapoarte confidentiale în legătură cu activitățile comerciale..."

"(...) Cercetările au dezvăluit că una dintre aceste întreprinderi a mers dincolo de spionajul industrial intrând din plin pe terenul extorcărilor, plecând de la informațiile compromițătoare pe care le obțineau prin intermediul ascultărilor telefonice ilegale".

"(...) Sunt exemple că s-a reușit obținerea unei duble rentabilități din aceste convorbiri telefonice interceptate (...). Pe de o parte era extorcat omul de afaceri al cărui telefon era ascultat, care era amenințat că vor fi făcute publice convorbirile sale. O dată încasat prețul șantajului, marfa era vândută din nou altor oameni de afaceri. Astfel, conținutul unei singure benzi înregistrate putea aduce beneficii incalculabile. (...) Această rețea nu se limita la ascultări ale convorbirilor telefonice ale persoanelor asupra cărora se dorea practicarea șantajului, ci erau realizate

mascat, și fotografiile ale obiectivelor controlate. În plus se obțineau tot felul de date asupra deplasării automobilelor celor spionați pentru a se realiza astfel un sistem de urmărire la înălțimea celor mai bune servicii de informații. Fără îndoială, faptul se datora implicării unui fost colonel al C.E.S.I.D. (Serviciul Secret Spaniol) (...), Fernando Rodriguez Gonzales (...)"

În numărul 6048 al cotidianului "El pais", din 19 noiembrie 1993, este publicat, articolul "*Mai mulți dintre arestați îl acuză pe contele de Godo că a ordonat acțiuni de spionaj*". Din conținutul acestui articol, semnat de F.Mercado și B.Cia, redăm următoarele:

"(...) În rândul înalților funcționari din Ministerul de Interne există felurite păreri. Secretarul de stat pentru Securitate, Rafael Vera, declară că 'în general se pare că nici un agent al C.E.S.I.D. nu este implicat'; el apără și dreptul foștilor agenți ai C.E.S.I.D. de a-și căuta un loc de muncă în sectorul privat în momentul în care părăsesc serviciul oficial. I se pare normal ca ei să-și caute acest loc de muncă 'în sectorul pe care îl cunosc, cel al securității'. Alții consideră că a fost desființată o rețea care dispunea de un potențial teribil, dată fiind capacitatea sa de a obține informații deosebit de compromițătoare de la oameni de afaceri și de a proceda la extorcări pe baza acestor informații. (...) "

Cotidianul spaniol "ABC", din 19 noiembrie 1993, publică articolul "*este posibil ca Tele 5, canalul de televiziune, să fi fost extorcat, plătind cu 20 de milioane o informație confidențială*". Din conținutul acestui articol, semnat de Dolores Martinez și Jose Clemente, redăm următoarele:

"Mai mulți dintre cei arestați pentru ascultările ilegale la Barcelona au declarat în fața judecătorului că președintele și editorul ziarului barcelonez 'La Vanguardia', Javier de Godo, a fost cel care a ordonat interceptării convorbirilor telefonice ale unor persoane din cadrul diferitelor mijloace mass-media. Pe baza acestor mărturisiri, magistratul care instruește cazul, l-ar putea cita pe contele de Godo pentru a răspunde acestor acuzații (...). În acest sens, Godo s-a oferit să colaboreze cu judecătorul pentru clarificarea chestiunii. Din primele cercetări, deocamdată fără confirmare, rezultă că: Miguel Ruiz Martinez și Manuel Maria Sanchez (foști agenți ai C.E.S.I.D.) au fost însărcinați să spioneze pe: Mario Conde, Jesus Polanco, Rafael Jimenez de Parga, Manuel Martin Ferrand și alte personalități. Cei menționați

în prealabil îi spionau și pe: Carlos Fajado Ricoma și Alberto Garrofe Pardo (foști angajați ai ziarului 'La vanguardia'). Fernando Rodriguez Gonzales (fost colonel în cadrul C.E.S.I.D.) era însărcinat să-i spioneze rudele lui Javier Godo, și pe cei din anturajul acestuia, pe cei de la ziarul 'La vanguardia', oameni de afaceri, alte personalități."

Motivele spionajului au fost:

- furnizarea de date C.E.S.I.D.;
- folosirea unor date pentru a extorca întreprinderile din

Madrid și Barcelona de la care obțineau, de la caz la caz, între 10 și 15 milioane de pesetas.

Mijloacele tehnice de spionaj au rezultat:

- ascultarea liniilor telefonice;
- microfoane plasate în diferite încăperi;
- filaj;
- acces la documente.

Au fost arestați:

- Fernando Rodriguez Gonzales (consilier în probleme de securitate al ziarului 'La vanguardia');
- Gemma Guillen (secretar al lui Godo);
- Miguel Ruiz Martinez;
- Manuel Maria Sanchez plus alte 11 persoane.

"În timp ce 7 dintre cele 15 persoane implicate au fost puse la dispoziția judecătorului, patru dintre acestea au intrat în închisoare, 2 au fost puse în libertate. Unii dintre cei arestați au afirmat că secretarul lui Godo, Gemma Guillen Lopez, avea cunoștință despre activitățile ilegale ale rețelei. (...) "

"Ieri s-a aflat că una dintre întreprinderile extorcate de această rețea a fost canalul de televiziune Tele 5, care a ajuns să plătească 20 de milioane de pesetas pentru o informație (...). "

"Surse provenind din cadrul celor care cercetează cazul au afirmat că au existat două activități de ascultări și spionaj. (...) În iulie, fostul colonel al C.E.S.I.D., Fernando Rodriguez Gonzales, a fost angajat de serviciul de securitate al ziarului 'La vanguardia'. În cadrul primei activități, Javier de Godo a ordonat cercetări asupra celor ce conduceau ziarul și asupra celor care îi făceau concurență. În cadrul celei de-a doua acțiuni, sursele îl definesc drept victimă pe Godo. (...) Majoritatea acțiunilor care leagă persoana lui Godo de acțiuni de spionaj au avut loc între anii 1990 și 1992. (...) În această perioadă, Antena 3, post de televiziune

aflat sub controlul lui Godo, și-a schimbat acționarii prin pătrunderea grupului Prisa, al cărui președinte este Jesus Polanco, editor al ziarului guvernamental <<El pais>>".

"Conform diferitelor surse, pentru securitatea sa personală și pentru a controla negocierile și contractele, (...) Godo i-a angajat pe agenții Cesid Miguel Lejarza Eguia, 'Lupul', care își ascundea identitatea sub numele de Miguel Ruiz Martinez, Manuel Maria Sanchez și Juan Rodriguez. Aceștia au creat în 1990 întreprinderea 'Strategic', destinată 'cercetărilor'. (...) Ulterior, aceștia au fondat întreprinderea 'General Consulting SA' (...)"

"Printre primele acțiuni cu care conducătorii ziarului i-au însărcinat era și o cercetare în legătură cu eventualele detournări de fonduri de care s-ar fi făcut vinovate anumite persoane având funcții de răspundere în cadrul ziarului".

"Înainte de a realiza această acțiune, respectivii au luat legătura cu o persoană importantă care i-a ajutat în interceptările posturilor telefonice. (...) În ianuarie 1992, 'personalul de securitate' al ziarului 'La Vanguardia' a sporit prin încadrarea lui Manuel Maria Sanchez, a lui Juan Rodriguez Gonzales și a lui Luis Izquierdo Guillean".

"Poliția a afirmat că cercetările în legătură cu această rețea de spionaj și extorcare nu sunt încă încheiate și au arătat că (...) arestările ar putea continua. (...) În afară de arestarea membrilor rețelei. Poliția (...) cercetează dacă spionii și excrocii din jurul lui Godo nu furnizau și C.E.S.I.D.-ului informațiile pe care le obțineau. (...) Această ipoteză a fost formulată în, virtutea unor cazuri anterioare similare".

"<<Spionul>> Alain Patterson, care conduce o întreprindere de aparatură electronică specializată în ascultări telefonice, a dat asigurări că la Barcelona există aproximativ 300 de telefoane sub control și că există numai 60 de autorizații judecătorești în acest sens. Aceste declarații dau la iveală enorma cantitate de ascultări telefonice ilegale, care se realizează în fiecare zi. 'Omul de afaceri - spion', de naționalitate franceză, a dat asigurări acestui ziar că C.E.S.I.D. realiza diferite înregistrări cu <<personalități foarte importante și puternice din punct de vedere economic, și al mass-medie>>".

"Nu este clar că mass-media în chestiune ar fi 'La Vanguardia', spionul putându-și referi la 'Observator', unde lucrau foștii directori de la 'La Vanguardia', Alberto Garrofe și Carlos

Fajado. (...) Spionul francez a declarat că 'există persoane pe care le interesează informații despre oameni cu funcții înalte, politice sau în afaceri care trec prin dificultăți financiare' (...). A afirmat că materialul pe care îl vinde întreprinderea sa este cumpărat de către Poliție și de către CESID 'cărora deja le-a îndeplinit diferite solicitări'. Alain Patterson a cunoscut multe dintre activitățile acestei rețele prin genul de material care îi era solicitat. << Când o anumită persoană îmi solicită un anumit 'chip' sau o instalație de înregistrare știu imediat în ce scop le va utiliza >>. În general - a adăugat el - nu adresez întrebări indiscrete în legătură cu ceea ce se află în spatele acestor chestiuni, însă știu despre ce este vorba și păstrez tăcerea".

Cotidianul spaniol "ABC" din 21 noiembrie 1993, publică, articolul "*Este posibil ca 'rețeaua Godo' să fi fost utilizată în războiul dus de către PSOE împotriva 'clanului catalan'*". Din conținutul acestui articol, nesemnat, redăm următoarele:

"Există indicii care arată că persoane cu funcții înalte din cadrul Executivului ar fi putut manevra rețeaua de ascultări telefonice din Barcelona cu unicul scop de a aduce prejudicii vicepreședintelui guvernului, Narciso Serra, în bătălia cruntă dintre familiile socialiste. Se bănuiește că, pentru a câștiga acest 'război', au fost folosite serviciile secrete care lucrau pentru Godo, se pare, cu intenția de a obține informații care să poată afecta așa numitul 'clan catalan'. Nu ar fi de mirare dacă benzile care se află la Poliție ar conține convorbiri cu mare însemnătate politică între președintele editor al ziarului 'La Vanguardia' și persoane deținând înalte funcții în cadrul PSC - PSOE, printre care s-ar afla, conform diferitelor surse, mai mulți miniștri și Serra însuși (...)"

"În timp ce unii dintre agenții C.E.S.I.D. se ocupau de filajul respectivelor personaje sau le ascultau telefoane pentru a obține informații compromițătoare, anumiți înalți funcționari trăgeau sforile în calitatea lor de ultiimi destinatari ai tuturor acestor informații, cu care se dorea compromiterea oamenilor forte din cadrul PSOE aflați la putere. Dacă prima dintre rețelele pe care se pare că le-a înființat Godo îl avea ca destinatar al acestor informații chiar pe președintele și editorul ziarului 'La Vanguardia', legăturile acestuia cu socialiștii catalani l-au făcut obiectul unor simpatii obscure pe care el însuși nu le cunoștea".

"Cineva 'aflat foarte sus în PSOE', este cel despre care surse confidențiale (...) au susținut că ar fi cel care 'trage sforile'.

(...) Aceleași surse precizează că rețeaua importantă (...) este aceea care utilizează informația pe care o primește pentru a-i înfunda pe unii și pentru a-i murdări pe alții. Vom vedea lucruri groaznice, asemănătoare unei 'răzbunări siciliene' (...).

"Aceste declarații, făcute confidențial ziarului 'ABC' de către persoane care cunosc cazul (...) nu exclud că 'rețeaua Godo' ar fi putut fi utilizată și de sectoare foarte influente din cadrul PSOE (...). Aceleași persoane au subliniat posibilitatea ca 'cineva care conduce acum în cadrul partidului și care a fost îndepărtat din guvern' să fi putut fi principalul beneficiar al informațiilor obținute (...). De asemenea este posibil ca, trecând timpul, ascultările acumulate să fi dezvăluit relații obscure între conducătorii PSC-PSOE și o mare urzeală financiară, străină, în ultimă instanță de interesele PSOE, fapt care ar fi putut fi folosit de către celălalt sector al partidului pentru a izola 'clanul catalan'".

"Sursele din apropierea celor ce întreprind cercetările nici nu confirmă, nici nu dezminț existența 'cuiva aflat deasupra celor arestați și a lui Godo care ar putea să beneficieze de toate informațiile'. (...) 'Omul din umbră' (...) s-a gândit că înainte sau ulterior unele persoane din cadrul PSC ar putea purta convorbiri compromițătoare cu principalul conducător al ziarului catalan. (...)"

"Cu toate că nimeni nu-l indică direct pe secretarul adjunct al PSOE, Alfonso Guerra, ca fiind, 'cel care trage sforile', este clar pentru toți că toate indiciile și toate bănuielile îl plasează în spatele întregii intrigi. (...) Sursele menționate reamintesc despre excelentele relații pe care Guerra le menținea în trecut cu serviciile secrete spaniole, precum și interesul său permanent pentru informații confidențiale, informații cu care obișnuia să-i amenințe pe liderii opoziției".

"Dacă pentru Guerra aveau interes conversațiile politice ale adversarilor săi, nu era mai puțin important pentru el să cunoască dedesubturile războiului întreținut de canalele de televiziune, pătrunderea în cadrul acestora a capitalului străin, precum și operațiunile financiare extrem de complexe care se desfășurau în jurul lumii, mass-media. Ambele chestiuni atrăgeau mult atenția unui om căruia, fiind marginalizat în cadrul puterii și izolat de un sector dominant în cadrul partidului său, nu-i rămăneau decât posibilitățile oferite de către feluritele rețele de

informații pentru a pătrunde până la rădăcina marilor afaceri care se pregăteau și care aproape ieșiseră de sub controlul său".

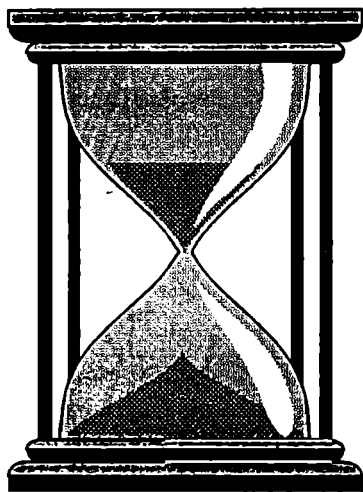
"Importanța grupului Godo nu-i era străină lui Alfonso Guerra. (...) Cineva i-a sugerat posibilitatea că, prin intermediul acestui grup, ar putea avea acces la un volum de informații care să-i înapoieze o parte din puterea pe care o pierduse în favoarea 'clanului catalan'. C.E.S.I.D. era singura cale prin care Guerra ar fi putut cunoaște în detaliu evoluția acestui grup și să riposteze la mișcările principalilor săi rivali din cadrul partidului".

"Sosirea C.E.S.I.D.-ului la 'La vanguardia' nu este întâmplătoare, tot așa cum nu era întâmplător faptul că fostul colonel care (...) a venit acolo știa, înainte de a sosi, că grupul Godo era cercetat de către propriul său serviciu de securitate. Surse provenind din grupul de anchetă au recunoscut, la fel cum au făcut și purtătorii de cuvânt ai ziarului, că nimeni dintre cei de la 'La vanguardia' nu avea nici cea mai mică bănuială că erau victimele monstrului pe care îl creaseră ei însăși".

"Săptămânalul spaniol "Tiempo" din 29 noiembrie 1993, publică articolul *"Rețeaua de ascultări ilegale a elaborat 'dosare' asupra lui Pujol și a lui Benegaz"*. Din conținutul acestui articol, semnat de Antonio Fernandez, redăm următoarele:

"'Ai grijă! Dacă mi se întâmplă ceva, tu nu mai ai de trăit nici măcar 24 de ore'. Fraza a fost pronunțată de către Miguel Luiz Martinez, un fel de detectiv privat, în fața unui cunoscut care (...) îl avertizase că unele dintre activitățile pe care le executa ar fi putut fi denunțate. (...) În realitate, Miguel Ruiz se numește Miguel Lejarza, poreclit 'Lupul'. Infiltrat în cadrul organizației teroriste ETA între anii 1973-1975, a favorizat căderea conducerii ETA și ulterior, cu o nouă identitate și cu un chip nou, a lucrat la ambasada spaniolă din Mexic. Pe data de 1 iulie 1987 a fost arestat deoarece extorcase un dentist basc în numele ETA și apoi a plecat la Barcelona unde a lucrat pentru diferite agenții de cercetări. Mai târziu și-a creat propria sa rețea de astfel de întreprinderi. Probabil că niciodată nu s-ar fi auzit despre el dacă pe data de 5 decembrie 1991 angajatul întreprinderii telefonice pe nume Gregorio Carrascal nu ar fi găsit (...) un microfon, conectat la telefonul lui Albert Garrofe, un avocat care în urmă cu două luni era unul dintre conducătorii ziarului 'La vanguardia'. (...) Fostul director financiar al ziarului 'La vanguardia', Carlos Fajado, era obiectul unui spionaj de același tip."

"Cercetările i-au condus pe polițiști la trei persoane care cumpăraseră 'microfoane' de acel tip: Miguel Ruiz Martinez, Jose Manuel Trujillo Ortiz și Manuel Sanchez, alias *Mariano*. În februarie, Ruiz Martinez și Trujillo Ortiz au fondat două întreprinderi: General Consulting Communication și Broadcast. Aceasta din urmă fusese creată, în mod oficial, pentru producția de seriale pentru cinematogafe și televiziune. Trujillo avea motivele sale pentru a întemeia o societate de acest tip: lucra pentru Javier de Godo, care era pe atunci președintele canalului de televiziune Antena 3. (...) Acestora li se adaugă colonelul C.E.S.I.D. - ului Fernando Rodriguez Gonzales, consilier în probleme de Securitate al lui Godo. Contactul tuturor celor menționați, cu grupul de afaceri al aristocratului catalan s-a făcut prin însuși secretarul lui Godo, Gemma Guillen. Aproape în același timp 'cădea' și secretarul personal al contelui, Jose Tomas Brenchat. Ulterior, alți doi colaboratori ai serviciului de securitate al ziarului s-au văzut implicați în cazul respectiv: Juan Gracia Navarro și Salvador Daroqui Gual, ultimul fiind șoferul lui Godo".



BIBLIOGRAFIE

1. The business of Spying de Brian Murphy
editat: Milton House Books - 1973 - London NW1
2. A comprehensive Report on Eavesdropping
Techniques and Devices and their Corresponding
Countermeasures
editat: Telecommunication Publishing Inc - S.U.A.
3. The interaction between communication privacy devices
(CPD) and communication system - 1975 de Arnold
M.McColmant
4. Dicționar tehnic de radio și televiziune de
dr.ing.N.Stanciu
editura Stiințifică și Enciclopedică
5. Science et vie
colecția 1990 - 1993
6. Culisele Palatului regal 1930 - 1940
de Neagu Cosma
editura Globus - București 1990.

 Tiparul executat la tipografia
OLIMP PRINTING SERVICES

